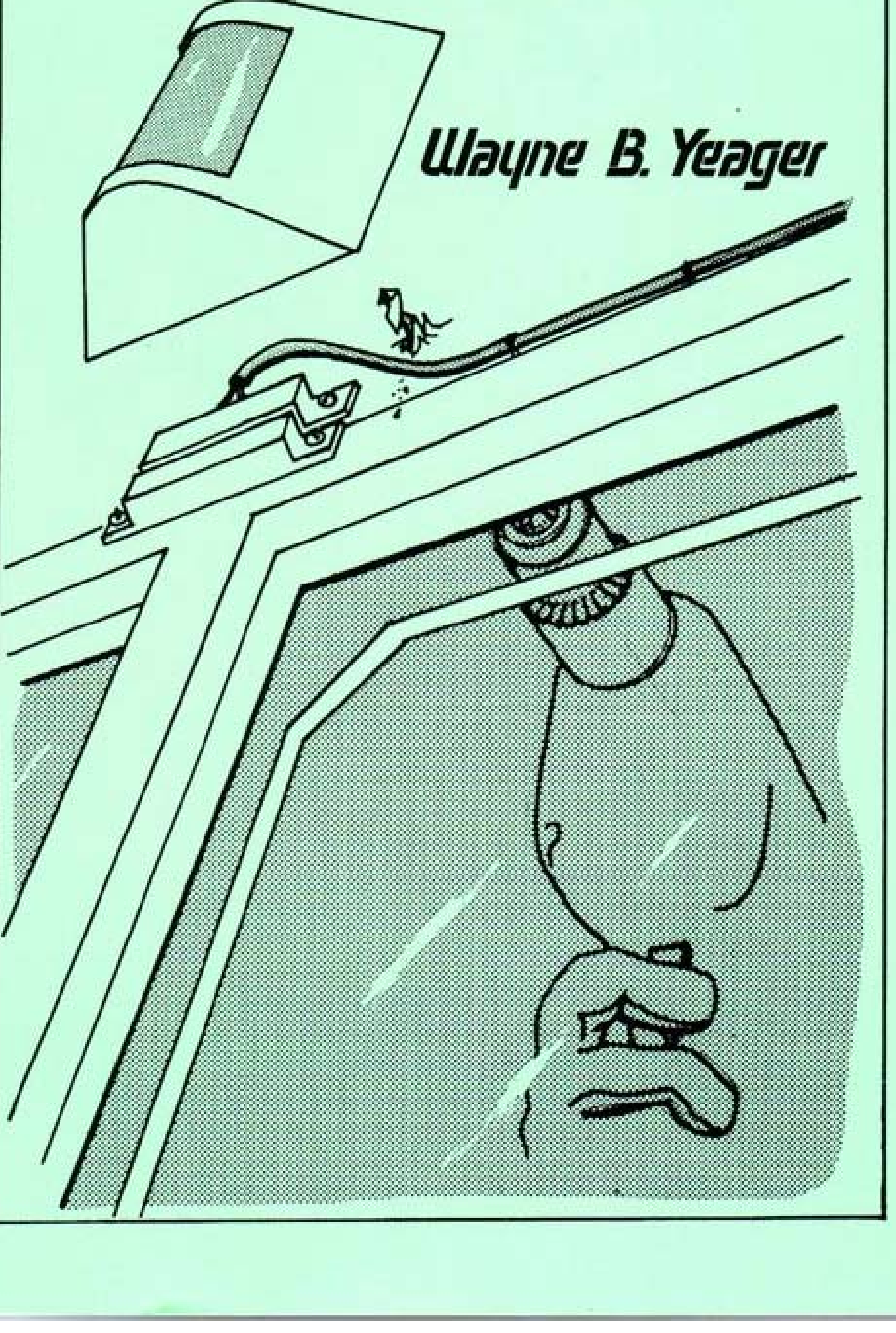
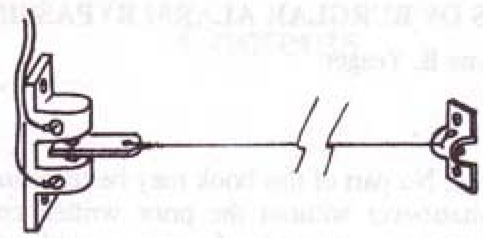
TECHNIQUES OF Burglar Alarm Bypassing

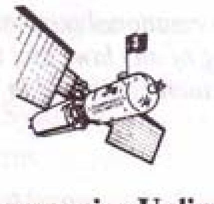
Wayne B. Yeager



TECHNIQUES OF
Burglar Alarm Bypassing



Wayne B. Yeager



Loompanics Unlimited
Port Townsend, Washington

TECHNIQUES OF BURGLAR ALARM BYPASSING

Published by:
Loompanics Unlimited
PO Box 1197
Port Townsend, WA 98368

Cover and Illustrations by Kevin Martin

ISBN 1-55950-032-8
Library of Congress
Catalog Card Number 90-60262

Contents

INTRODUCTION

One does not need to be a professional thief or aspiring burglar to reap benefits from this book. Although it sometimes reads like a How-To manual, it was written primarily to show homeowners their vulnerabilities, to teach law enforcement officials some tricks of the burglar trade, and to inspire burglar alarm manufacturers and installers to seek new methods of deterring and detecting burglary. This book does not give professional burglars any information that they do not already possess, and I believe that society is best served when information is available to all, rather than to a select few. Burglar alarm jumpering and bypassing is mere tradecraft for the professional burglar, but printed information on the methodology of this rare science is scarce, to say the least.

Burglar alarms are always installed for one reason: to protect something. Whether it's valuables, one's life, items of sentimental value, etc., the objective of the burglar alarm remains the same. Long ago, people used the safety of high walls and castles to protect themselves and their property. Later, the key-lock was invented to protect valuables, and today we have high-security locks, vaults, and alarms. Human guards have been used throughout history to protect

assets, and the modern burglar alarm is simply a guard made of electronic components. But like its predecessors, it too is fallible.

Every now and then, a new technology emerges which finds its way into the security industry. For example, the Passive Infra-Red alarm system commonly in use today was a by-product of the research on heat-seeking missiles conducted by the military. But just as technology marches on towards the good of mankind, so too does it march for the resourceful crook. One can be certain that the state-of-the-art alarm system that is installed today can be bypassed tomorrow, for criminal technology is constantly on the heels of security technology. From the first "unpickable" lock ever picked, to the "fool-proof" bio-mechanical systems being compromised today, the evidence is overwhelming that "absolute security" exists in theory only.

We shouldn't discount the value of burglar alarms, however, for they do earn their keep. They often catch the impulse thief, the crow-bar-wielding amateur who risks jail for a VCR or television while ignoring the original Renoir on the wall. They also deter the advanced amateur, who, realizing an alarm impedes his progress, opts to try somewhere else where no alarm has been installed. And frankly, they increase the chance that a professional burglar will be apprehended, but for him, this is a calculated risk. He knowingly accepts this risk, just as an astronaut accepts the inherent risk that accompanies space travel. However, unlike the unlucky astronaut who pays for his mistakes with his life, the professional thief knows that even if he is caught, he will serve, according to national crime statistics, an average sentence of only one year and nine months.

The actual number of professional burglars is probably very low, and unless you own something of extreme value, it is unlikely that you will become the target of a professional. Therefore, a professionally installed burglar alarm system will probably be more than enough for your security needs. If, however, you have valuable possessions that make you a candidate for a professional burglary, you should remember this one axiom: no system will stop an intelligent and determined burglar if he wants your possessions badly enough.

I have worked in the security industry for years, and I've seen most of the alarm components and systems in use today. I've also dis-

covered ways to bypass many of them. Some methods are admittedly crude, but others are quite crafty. I have not attempted to include every technique of bypassing alarms in this book, because new techniques are constantly being discovered, and it would be quite impossible to explore every possibility. I have, however, included the most common ways that burglars defeat our attempts to protect our homes and businesses.

In closing the introduction, I would like to remind the reader of a fact that at first glance seems paradoxical. That is, as burglar alarms become more and more sophisticated and complicated, the less and less secure we actually become. The reason is because we begin to put too much faith in them, and soon we are convinced that our homes and businesses are burglar-proof. We tend to subconsciously instill the system with the ability to catch burglars, and we automatically assume that the system will compensate for our laxity. As a result, our entire security is placed in the hands (or chips) of a machine, and machines are much more susceptible to compromise than are humans. As you will see, a magnetic switch does not "know" when a door or window is opened, it merely detects the absence of its companion magnet. A Passive Infra-Red Detector does not "know" when an intruder enters a protected room, for it simply detects the changes of temperature within the room. Therefore, any situation that is necessary can be manufactured, and the component can be made to "think" that all is well.

An alarm is a very useful tool that every homeowner, rich or middle-income, should own. It will protect you and your valuables from all but the most determined thief. An alarm system allows for an incredible peace of mind, and it is an asset when selling a home. However, a burglar alarm will not provide an impenetrable barrier behind which you and your family can hide, as this book will prove.

PART I

Burglar Alarm Systems

Part I is an introduction to the various types of alarms in use today. In the first chapter, hard-wired protective circuits, the most common, are discussed. These are the circuits that guard a building's perimeter. Therefore, they are used primarily on doors and windows. The most common member of this family is the ubiquitous magnetic switch, the little set of white rectangular boxes seen above the doors of most businesses. The second chapter deals with the second line of defense, the area sensor. These sensors monitor a specific area rather than a specific point of entry. These are often called motion detectors, since anyone moving about a guarded room will be detected. The manner in which these sensors achieve this goal varies between components. The third chapter offers some general notes and observations on alarm bypassing before the examination of specific components begins.

1

Protective Circuits

The Protective Circuit system is the most common alarm apparatus in use today. Therefore it is imperative that you fully understand the principles involved. The premise of the protective circuit is that if a closed circuit suddenly becomes open, or if an open switch suddenly becomes closed, an alarm will sound. Look at Fig. 1-1 (see page 8). The electric current is travelling throughout the entire circuit at near light-speed, from the batteries through the wire, to the switch, to the control panel, and to the batteries again. This is known as a protective circuit. The current will travel throughout the circuit as long as there are no interruptions. But let's say the switch gets pulled apart. See Fig. 1-2 (page 8). Now, the control panel's electronics tell it that the circuit is no longer intact, and a relay sends power to the bell which makes it ring, thus announcing an intrusion. This method of monitoring is known as hardwiring because all components of the alarm are connected by electrical wire, as opposed to wireless alarms that transmit their signals to the control panel. (These are discussed in Chapter 2.) Basically all hardwire systems contain magnetic switches on doors and windows, a control panel to which they are connected, batteries for power, and a loud bell or siren. For the sake of simplicity,

I've shown the circuit below with only one switch. However, most alarms have several, sometimes dozens, of different switches to cover all possible points of entry.

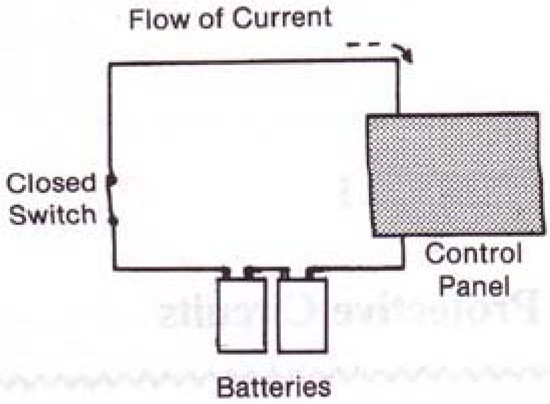


Figure 1-1

A protective circuit alarm in the closed position.

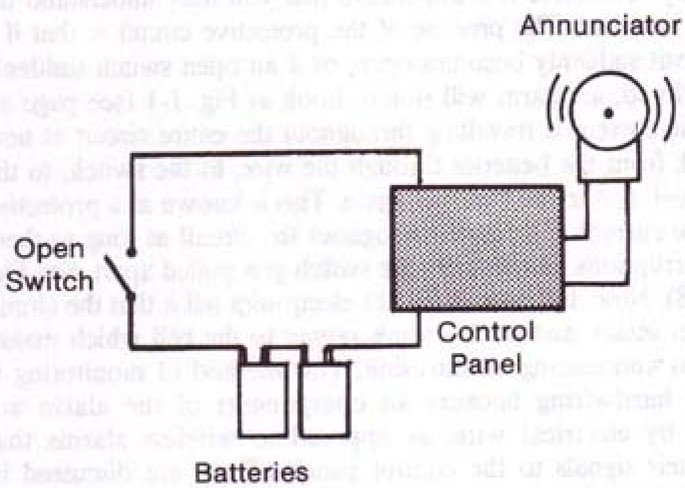


Figure 1-2

The alarm is triggered when the switch is opened.

In Figure 1-3, you can see an alarm system containing six different switches. In an average home, we could dedicate two of these to our front and back doors, and the other four to first-floor windows. A violation on one of these six points of entry would trigger an alarm signal. Electricity is a curious thing, however. Note the flow of current in Figure 1-3. The current must flow throughout the entire series of switches before it returns to the batteries and control box. If a clever burglar were to place a "jumper wire" across the circuit (see Fig. 1-4 on page 10), the circuit would remain intact, and the panel box would be none the wiser. The thief could then violate switch after switch without setting off an alarm because electricity always follows the shortest path to complete the circuit, when given a choice.

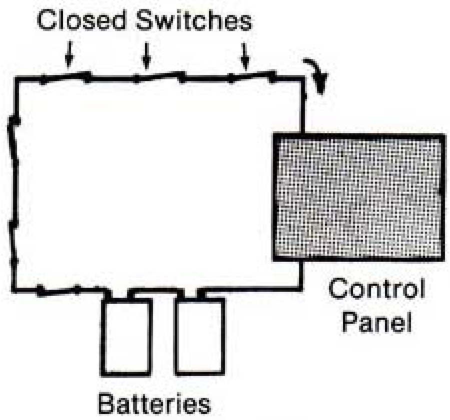


Figure 1-3

A protective circuit alarm with a switch for each protected point of entry.

So it would seem that all a thief must do is locate the wires to and from the circuit, and jumper them to bypass the entire system. While the theory is true enough, it is a bit more difficult in practice. Jumpering is still fairly common when bypassing basic components and the cheap do-it-yourself burglar alarm kits, but becomes much more difficult when the thief encounters professionally installed

systems. Wires are usually hidden under floors and in walls, and often phony wires, that do absolutely nothing, are combined with the real ones to throw a would-be burglar off track. Also, the batteries are usually strategically placed somewhere within the circuit (other than the control panel), so that even if the correct wires are found, an attempt at a jumper near the control box would fail, because the lack of power will not complete a circuit. If that's not enough to dissuade an intruder, alarm manufacturers, in their constant state of paranoia, have installed in many high quality panels, an end-of-the-line resistor. This measures the constant specific resistance in the circuit. If any change in this resistance is apparent, due to jumpering, for example, an alarm will still sound. One way burglars get around this inconvenience is to place on the jumper wire itself a potentiometer or variable resistor. After the resistance of the circuit is registered on a multimeter, or an ohmmeter, the jumper's potentiometer would then be set to that resistance, and the "jumper-er" hopes for the best. However, the end-of-the-line resistor is sometimes so sensitive, that even the smallest change will trigger an alarm. So obviously, this method would work only on an end-of-the-line resistor whose tolerance is rather lenient.

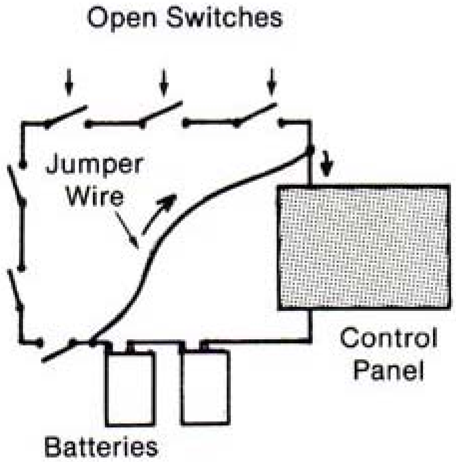


Figure 1-4
A jumper wire defeats the alarm by keeping the circuit closed.

Jumpering is a very common method of burglar alarm bypassing, and is the method of choice for the semi-sophisticate. However, it only works on a totally hardwired system, and is very unreliable due to some of the modern safeguards. Sometimes before reaching a suitable jumpering point, one must violate a switch in the process, thus defeating his own purpose. But there are many more effective methods of bypassing this system, as you will see in later chapters.

2

Area Sensors

The other type of alarm system that we'll cover is known collectively as "Area Sensors." Unlike protective circuits, that cover only specific points of entry, the area sensor, or motion detector as it is sometimes called, is relied upon to monitor large rooms or even whole buildings. This type of system erects invisible barriers that must be penetrated in order to enter or move about the area. These barriers are not easily defeated, and are sometimes difficult to detect.

If Mr. Wilson owned a large retail store, he could probably keep most criminals out with electrified fences, bars on the doors and windows, and several Dobermans in the parking lot. But if a thief hid himself in the store during business hours, he could pilfer at his leisure after business hours. Mr. Thief would not violate any perimeter alarms, get electrocuted, nor get bitten (until he left, that is). However, with the advent of area sensing devices, the thief that tried this trick at the local K-Mart would have to be pretty sneaky. If he makes a noise, has a body temperature greater than sixty degrees, has conductive skin, or is made of matter, he will more than likely set off an alarm.

All this is very disheartening for Mr. Thief, but very good for Mr. Wilson, the store owner. For now he can install an area-sensor system that is more reliable than the Dobermans and electric fences at a fraction of the cost.

Sometimes these detectors transmit their signal to a centralized control panel within the home or business, and can be used in conjunction with a hardwired, protective-circuit system. Many systems allow you to directly incorporate the motion detectors into the line of the circuit, so that when the sensor "senses" something, it opens (or closes, depending on the system) a switch, just as a door contact would.

The list of obvious advantages of this system is enormous. One could monitor a room containing sensitive documents, or overlap many of them to cover several acres. Thus, the primary benefit of this generation of security system is the relatively inexpensive cost involved in monitoring large surface areas. Although they are impractical for guarding single objects, such as a painting, they are sometimes used inside safes and vaults just in case the other methods of detection and deterrence have failed.

Because of the nature of these systems, motion detectors cannot, of course, be used where motion frequently occurs. Dog and cat owners who keep their pets indoors are generally excluded from using area sensors, because animals are notorious for creating false alarms. The false alarm is the primary disadvantage of the area sensor system. A heat-duct may blow on a heat detector, wind may set off a sonic alarm, a fire engine's siren may set off a preamplifier, a dog in the parking lot may cause a microwave system to go into an alarm condition, and countless other harmless things can happen to compromise the reliability of area sensors. It is better, I suppose, for these alarm systems to be over-sensitive rather than under-sensitive, but herein lies the opportunity for the imaginative burglar.

There are six types of area sensors that we will discuss in depth in Parts II and III. These are the passive Infra-Red system, the ultrasonic unit, the microwave system, electric eyes, proximity sensors, and preamplified microphones. Explicit instructions will be given in later chapters on how burglars detect and defeat each of them.

3

Random Thoughts On Alarm Bypassing

Alarm bypassing is an art form that is over a century old. Shortly after Alexander Pope patented his electromagnetic contact alarm in 1853, thieves learned that they could get around this inconvenience by simply cutting the wires. And since 1853, members of both sides of the law have been running neck and neck in their struggle to conquer the other. Amazingly, after nearly 140 years, the most common perimeter alarm in existence today is still the Pope electromagnetic switch, although slightly modified. The only real advance has been the advent of interior alarms, or area sensors, and they have been introduced in just the last three decades.

The chief drawback of any alarm system is its presumption that the burglar will enter in a conventional manner. That is, the owner of a perimeter alarm system believes that since he has guarded the windows and doors, an entry is impossible without the perimeter alarm knowing about it. However, an enterprising thief can enter a house *anywhere* by making his own door with a sledgehammer and chain saw. Walls are certainly psychological deterrents to most, but a professional knows that between he and your home lies only smashable bricks and cuttable wood. Granted, you probably won't see the old

sledgehammer/chainsaw ploy used in downtown Chicago, but it is quite possible that it happens every day in Suburbia, USA.

While the sledgehammer and chainsaw have their uses, there are many more tools that the professional burglar possesses. He may have a lockpick set, door-jamb spreader, glaziers' and wall climbing equipment, miniature transmitters, Infra-Red goggles, and bolt cutters, just to name a few of the big-ticket items. He certainly has many smaller tools that he can use on certain occasions, such as glass cutters, Ultra-Violet marking chemicals, handcuff keys, and pry bars. Using these tools and others, he always takes the path of least resistance to accomplish his objective. Which brings us to the most important tool in the burglar's arsenal: planning.

Planning is only possible after careful and deliberate study of the proposed target. Of course, a burglar never knows what he will come across, but it helps when he has eliminated several possibilities. For example, if the burglar is certain that he can enter through the doorway, he will leave the unnecessary equipment, such as glaziers' equipment and chainsaw, at home. With proper reconnaissance and planning, it is not even necessary for a burglar to worry about alarms. If a thief was certain there was a valuable painting in someone's second floor bedroom, could he break through a window, run upstairs, grab the painting, and leave before the police arrived? Most assuredly he could.

The other elements of alarm bypassing, besides planning, are detection and execution. Detection is important because one cannot bypass an alarm if he does not know it is there. Detection is most easily, safely, and effectively accomplished prior to the execution. This is, of course, not always possible, so in Parts II and III, I'll show on the spot methods of detection that thieves often employ. But sometimes, under the guise of customer, insurance salesman, potential client, etc., a burglar may "case" a home or business for the upcoming burglary. Also, there are methods of "preventive bypass" to counteract invisible, but possible alarms, but they are usually time consuming and burglars rarely depend on them. Examples of this are cutting holes in doors to avoid having to open them, or "walking a tightrope" to avoid stepping on a carpet that may contain a pressure sensitive mat. A pro-

fessional burglar maintains the state of mind that anything can be a trap, and he always acts accordingly.

After planning and detection, comes execution. This is accomplished by knowing the pitfalls of the alarm component. Detailed instructions for thwarting these components are contained in Part II, but they are by no means complete, for new methods are always being created by resourceful burglars. Execution can mean getting around an alarm component, or it can mean shutting the entire alarm system down. Almost every day, a person "legitimately" turns off his alarm system. This is done because he comes home from work, or because he is opening his store for business, and in either case he no longer needs an alarm. But because these systems can be legitimately turned off, they can also be "illegitimately" turned off, as will be explained in Part III.

PART II

Local Alarm Bypassing

In Part II, we will examine each component of a local alarm system, and see the most common ways of detecting and defeating them. A local alarm system is one that rings a bell, sounds a siren, or in some way notifies everyone in the surrounding area that a burglary is in progress. A monitored alarm, which is discussed in Part III, contains all the components of a local alarm system, except that it is silent to the burglar. Instead of bells and sirens, it secretly sends a signal to the police, alarm company, or guard agency.

The advantage for the burglar in bypassing local alarms is that he will know immediately if he has made a mistake, for the clanging of a bell is the giveaway. And, unlike a monitored alarm system, he needs only to bypass the necessary components instead of the entire system. Furthermore, the local alarm offers as many or more avenues of circumvention as does the monitored system, as you will see.

4

Silencing The Annunciator

There are two basic parts to every local alarm system in use today: the sensing device that detects the intruder, and the annunciator. If either part is nullified, then so is the entire system. The annunciator of an alarm system is generally a bell, siren, buzzer, horn, or other loud device (see Figure 4-1). It is meant to let everyone in the immediate vicinity know that a burglary is in progress. The problem is, most people simply ignore bells and sirens when they hear them on a busy street. Most homeowners, however, have told their neighbors that a bell or siren means trouble, and to call the police. If police happen

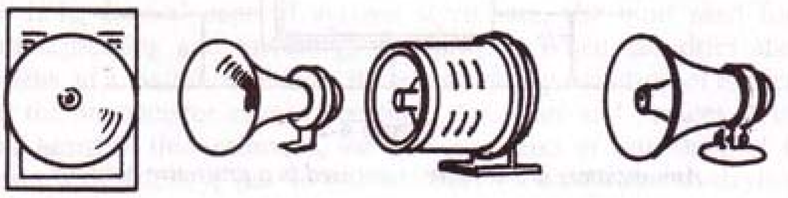


Figure 4-1
Alarm system annunciators.

to be in the area when the alarm sounds, they usually become momentarily confused. That is because in a large subdivision, it is difficult to pinpoint the origin of the clangor, due to echoing.

The annunciator is usually on the outside of the house or business, so as to raise the most commotion, although occasionally one is also placed indoors.

Locating the annunciator is relatively easy. It is nearly always very high on the sides or back of the house or business. It is either surface mounted or semi-flush mounted, and may even be encased in a protective housing (see Figure 4-2). This protective housing will have small slits to allow the sound to escape, and is nearly always protected against tampering. Any attempt on the part of the burglar to tamper with the door or wires, will generally result in an alarm condition. A good annunciator will also have a relay and a tiny generator that will power the bell if someone tries to cut off the electricity. The housing may be key-locked, to allow for easy maintenance (see chapter 13 for lock information). As I pointed out earlier, no components of a local alarm need to be bypassed if the annunciator can be properly disabled.

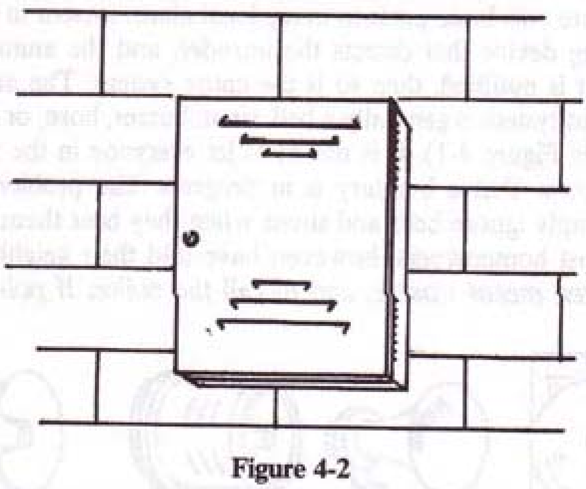


Figure 4-2
Annunciators are sometimes encased in a protective housing.

The first goal of the burglar is finding the annunciator. If it is not immediately visible, he may purposely set off an alarm so that he may

discern from where the sound is emitted. This is also a good opportunity for the thief to time the arrival of the police, at a safe distance of course. Once the bell or siren is found, the problem of getting to it arises. A ladder, in rural areas, may suffice, but carrying a ladder to a strange house is slightly conspicuous. Burglars prefer to climb the wall if possible, or climb a rope ladder that has been thrown onto and attached to the roof by a grappling hook.

However the annunciator is reached, the next step is to attempt to disable it prior to the housebreaking. Burglars often take the precaution of wearing ear-plugs or headphones, such as the kind hunters or shooters use. There is nothing quite as startling as holding onto a rope while 120 decibels suddenly pour into your ears. By the way, 120 dB, which is well into the pain level, is quite common for alarm sirens. Prolonged exposure at this stentorian level, will certainly cause permanent deafness.

If the annunciator is an exposed bell, the clangor may be snipped off with bolt-biters, or removed with a cutting torch. A small buzzer, like the fire alarms in schools and hospitals, is easily knocked off the wall with a sledgehammer if it is done quickly and forcefully. An exposed horn can be filled with modelling clay and tamped tightly, to decrease the audio output. A siren may also be filled with clay, but thieves have learned that the entire siren, inside and out, must be filled completely, or sound will escape through the sides. Many times, the older and/or cheaper models will even have a simple on/off switch on them.

If the annunciator is housed in a steel box, it is easily silenced without removing the door. The housing often contains small slits or louvers, but if not, a small hole can be made with a portable drill. Into this hole, several cans of aerosol styrofoam, the kind used for weatherproofing and insulating, are sprayed. When this dries and hardens, in a matter of minutes, it creates a nearly sound-proof barrier that the annunciator cannot penetrate. Amateurs and novices, who have heard of this technique, use shaving cream or something of a similar consistency, but it is less effective than the fast-drying insulation foam.

If the larceny is to be perpetrated later in the week, or perhaps the next day, an even more reliable method may be used. Instead of the

small hole, a larger one, about 1″ in diameter, is bored into the top of the steel housing. Very dry concrete, made without gravel, is then introduced into the hole using a funnel or a cake decorator's bag, until the entire housing is filled completely. Similarly, there is a liquid that pours like water, and hardens like glass in a few minutes, and is marketed under the trade name, Castolite®. Wax is also a possibility, but a heat source is obviously required. There is a slight danger in using these techniques, because liquid containing water is conductive. The introduction of concrete or any other liquid into the annunciator housing, may result in a closed switch, sounding the bell or siren. It would be somewhat muffled, of course, but sound would be emitted, nevertheless. Another possibility, although I've never seen or heard of it being done, is to actually build a muffler around the annunciator, and fill it with a suitable sound-proofing material.

If none of the above ideas are appealing, one may remove the bricks or siding surrounding the inexpensive annunciator, and search for any wires. If they are all cut simultaneously, the annunciator shouldn't annunciate, provided that the wires that are cut are the real ones.

When sound travels from an object, it decreases in intensity exponentially. A 120 dB annunciator is perceived to be only 95 dB at a distance of ten feet, and at one hundred feet, the decibels will have dropped tremendously. Considering that the nearest house or business will be about twenty feet away, the alarm signal will appear significantly fainter than it would at the source. If the burglar had an accomplice operating an air-powered jackhammer (that averages 97 dB) in front of the neighbor's house, an alarm signal would probably go unnoticed. If two accomplices were operating jackhammers, the effect would be even more profound. Of course, they had better have pretty good pretexts in case the neighbors wonder why in hell they're tearing up the sidewalk. Of course one may have three, four, or five accomplices with jackhammers, but the potential payoff would have to be pretty large for anyone to go to that much trouble.

5

Magnetic Contact Switches

The magnetic switch, the most common of all hardwired components, is found on doors and windows around the world. It consists of two individual pieces, the switch itself, and the companion magnet (see Figure 5-1 on page 26). The switching mechanism is a spring loaded lever that makes contact with a stationary metal arm when the companion magnet is near. Thus, the magnetic switch is a normally closed circuit. When the magnet is pulled away (see Figure 5-1 on page 26), the lever is released from the stationary arm and the circuit is no longer complete. So, the opening of a protected door or window removes the magnet from the switch, and, since the circuit is no longer complete, the alarm sounds. Since the circuit of a magnetic contact switch is normally closed, wires cannot be cut to defeat the system, for this has the same effect as removing the companion magnet.

The magnetic switch offers more opportunity for jumpering than does any other individual component. Since the wires are often visible, one needs only to remove the insulation, and place a small wire across the circuit to defeat and bypass the switching mechanism (see Figure 5-2 on page 27). The main problem for the thief then, is simply locating the wires, if they are not visible. Often they are hidden behind

baseboards or trimming, or are snaked through the studs behind the drywall. They may be uncovered from the outside, after the bricks and wallboard have been removed.

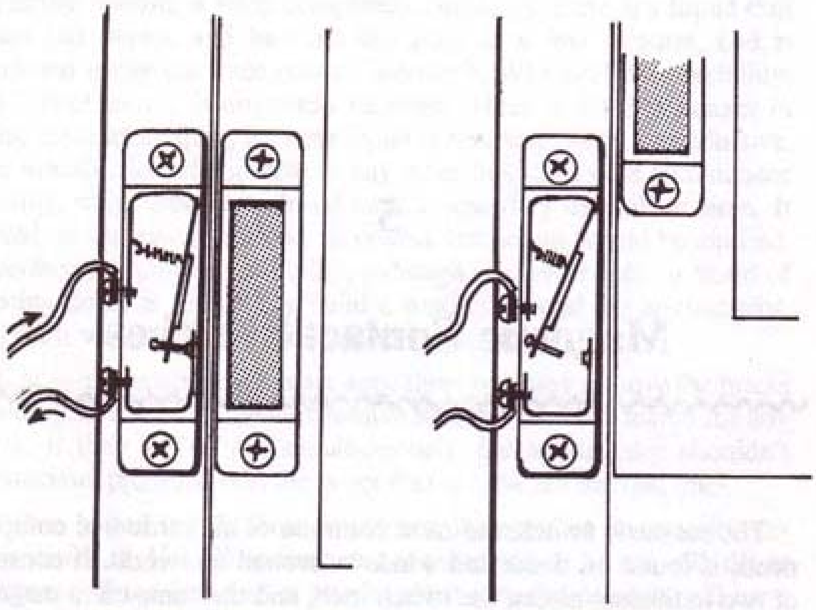


Figure 5-1

A common magnetic switch. On the left, the circuit is closed. When the magnet is removed (right), the circuit opens and triggers the alarm.

Usually, one has to already be inside to get at the wires, however there are a few tricks that burglars employ. A hole may be drilled or cut in the door or window, and a fiberscope may be inserted. A fiberscope has a viewer and a long flexible tube that allows one to see around corners and into small places. They are used primarily by doctors and electricians, but they also make an effective instrument for bypassing magnetic switches. If, after inserting the fiberscope, there are visible wires on the inside, another larger hole can be made through which an arm will pass. By watching the procedure through the fiberscope, the wires are easily bared and jumpered. The door can then be opened without creating an alarm condition.

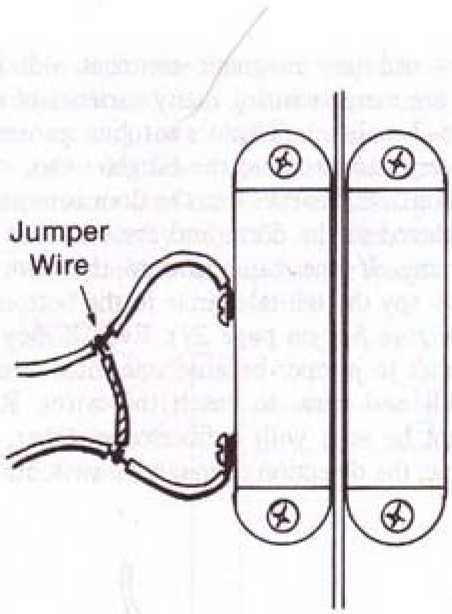


Figure 5-2

The magnetic switch is vulnerable to jumpering. The jumper wire maintains a closed circuit.

Of course, if one is going to cut a small hole, and then a larger one, a person could just cut a really huge hole in the door and crawl through it. But this is a bit more difficult with windows, because they are sometimes too small to crawl through, and because they may also be utilizing window foiling (see next chapter). But often, a hole can still be drilled in the window, and jumpering accomplished if the wires are visible. One way to make the wires visible is to unscrew the switch and give it a little pull. The wires will probably be stapled and may be difficult to pull, but there is a small chance that the wires were just stuffed in between the studs. This is done carefully so the switch is not removed too far from the magnet. One may also cut the drywall located behind the switch in an attempt to locate the wires. Also, if possible, the magnet may be unscrewed from the window itself and taped to the switch. The window could then be freely opened.

Since the visibility of ordinary magnetic switches aids in their defeat, some companies are manufacturing many varieties of recessed switches (see Figure 5-3 below). These switches generally go unnoticed, and can be very dangerous to the burglar who, after not seeing the old magnetic contacts, believes that the door is unprotected. The magnet is usually placed in the door, and the switch is usually recessed in the door frame. If one has access to the door during "normal hours," one may spy the tell-tale circle in the bottom of the upper door frame (see Figure 5-4 on page 29). Even if they can be seen, they are very difficult to jumper because one must remove, or cut through, the drywall and trim, to reach the wires. Recessed magnetic switches cannot be seen with a fiberscope either, so that brings us to our next topic, the detection of magnetic switches.

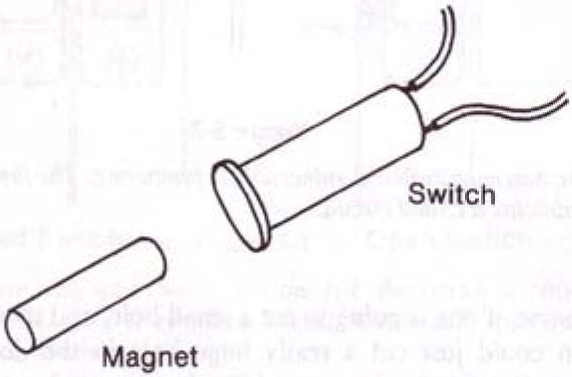


Figure 5-3
A modern recessed magnetic switch.

A high-quality liquid filled compass will react wildly when in the presence of a magnet. One placed near a door or window will certainly tell the user if a magnetic switch is nearby. After a compass has determined that a magnetic switch is indeed there, a gaussmeter

can be used to determine the exact magnetic strength. A magnet with the same strength and field is sometimes used to quickly replace the old magnet, making the switch none the wiser. A gaussmeter is very expensive, and very few systems outside the realm of high-security utilize bias sensors that sense different magnetic fields. So a gadget available through many scientific suppliers, called a Magnaprobe, will work in most situations to pinpoint the magnetic switch.

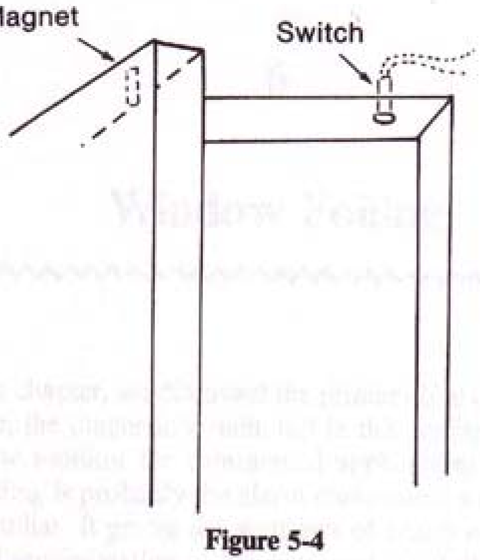


Figure 5-4

A recessed switch implanted in door and frame. This switch is very difficult to jumper.

In any of the cheaper versions that do not monitor the specific magnetic strength, but just need any magnet to hold the switch together, a super strong magnet will suffice. Burglars often use a Neodymium-Iron-Boron composite, which makes for a very efficient magnet; a NIB magnet the size of a quarter has a lifting power of about ten pounds. It is often affixed to a coat hanger and manipulated inside the premises, near the switch. The magnet is carefully maintained in such a way that it closely resembles the position of the old magnet. The door or window will then probably open without complications.

If a burglar doesn't know, or care to use, any of the above techniques, he will probably just cut a hole in a suitable place, and simply crawl through.

6

Window Foiling

In the last chapter, we discussed the primary line of residential window defense, the magnetic switch, but in this chapter, the most common window monitor for commercial applications will be covered. Window foiling is probably the alarm component with which laymen are most familiar. It graces the windows of nearly every liquor store, grocery, and service station in America, and rightfully so, for it is very difficult to bypass successfully. In the past, the unsightliness of window foil effectively kept it from widespread residential use, however, modern homeowners are becoming increasingly concerned with security, even at the expense of beauty.

When a window is to be monitored by foil, the foil is stretched around the perimeter of the window (see Figure 6-1 on page 32). Two "take-off blocks," or terminals, are placed at the end of the foiling and connected to the rest of the circuit. The foil, now part of a normally closed circuit, is so fine that if a break occurs in the glass, the foil will tear, opening the circuit.

Foiling is often coupled with magnetic switches, and there lies the big problem for the burglar. If he cannot raise or break the window,

how can he enter? The easiest way of bypassing this component is to simply avoid it and try entering somewhere else, but there are a few possibilities for the determined thief. There are three primary methods that burglars employ when defeating window foil. Amateurs, on the other hand, who don't fully understand the principles of a window foil circuit, try some crude methods that are usually unsuccessful. They sometimes smash the window, and hope that the foil won't break as well. The odds of this happening are astronomical since the foil is very tightly stretched, and breaks at the slightest provocation. I've even had to repair foil that had torn during a simple wind gust. Amateurs even try cutting the entire window out, since it allows them to get at, and jumper the terminals. But any slight movement in the wrong direction sets off an alarm (while they're holding a 20 pound sheet of glass).

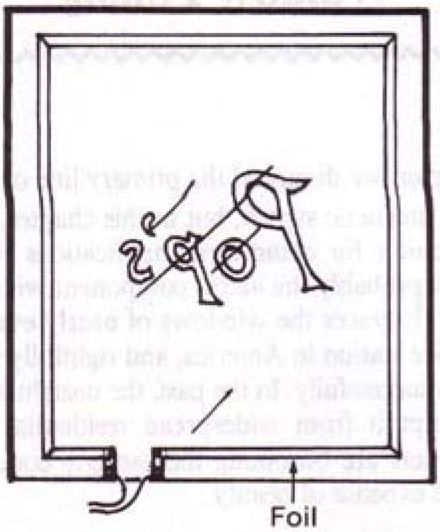


Figure 6-1

A ribbon of thin foil is stretched around the perimeter of a window. Any tear in the foil triggers the alarm.

One method that will work, provided the window is large enough (or the burglar is small enough), is the cutting of a crawl space in the

window that is far enough from the foil that it remains undisturbed. The entire window is covered with a strong duct tape, leaving blank the hole intended to be cut. The hole, preferably square, is scribed with a high-quality diamond tipped glass-cutter. The cutter is then used to trace and retrace the scribed lines until the glass gets quite thin. When the lines have been determined to be deep enough, a thin layer of modelling clay is applied to the glass area that is to be removed. Then, a thick, wet newspaper (to shield noise) is laid over the potential hole and tapped sharply around the scribed lines. With any luck, the glass will break only where the lines were cut. The duct tape serves as a shock-absorber, and also keeps the glass from shattering and falling to the floor if a mistake is made. The layer of clay serves to deaden the sound of the glass as it hits the floor inside.

Another method often used is the jumpering of the two foil terminals. If they are visible, a small hole is drilled into the glass near them, using a carbide bit. A wire is then laid across the terminals to completely bypass the whole foiling system. The wire is, of course, fastened securely to the terminals to avoid having it fall off during any part of the mission. A more reliable method involves baring the wires coming from each terminal and jumpering them. This is obviously difficult, since many times the wires are not visible, and since one is attempting it through a small hole. At any rate, if jumpering is successfully accomplished, the entire pane of glass can be shattered without setting off an alarm.

The third method is utilized when one has prior access to the premises. When no one is watching, a razor blade is used to surreptitiously cut a small piece out of the foil. The piece is just large enough that the circuit is no longer intact, but small enough so that it is not immediately perceptible. When the owner decides to arm (turn-on) his system, he discovers that the zone covering the windows will not arm properly (zones will be covered in detail in later chapters). After a quick survey of all the window foil, he figures that the system must be malfunctioning, and decides to arm every zone *except* the windows, and to call a repairman first thing in the morning. If this occurs, the window containing the cut foil will remain unguarded all night. It is conceivable that the owner could call a repairman that instant, but the intelligent burglar will be keeping his

eye out for that. If the owner finds the tear, there is really not much he can do without the proper tools and supplies. From the burglar's vantage point, he should be able to observe any repairs the owner is making on a particular window, and act accordingly.

Finally, it is also possible that the wires going from the terminals to the rest of the circuit, may be jumpered (see Figure 6-2 below). They may be uncovered by removing the bricks or siding, and cutting through the wall board. If the wires are revealed and jumpered, the entire window may be smashed without sounding an alarm. It is important to remember, however, that the jumper wire must have a shorter overall length than that of the original circuit.

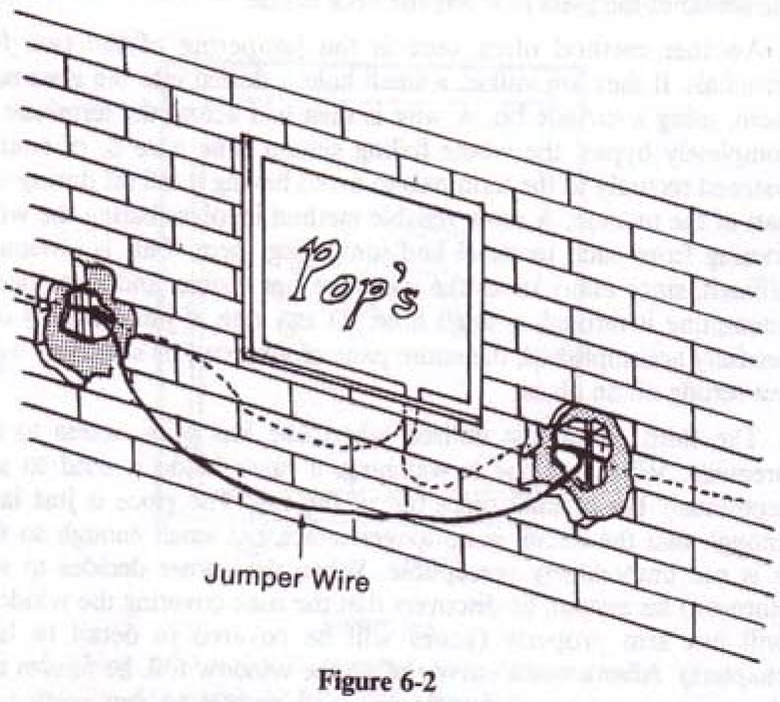


Figure 6-2

Window foil can be defeated by uncovering and jumpering the circuit wires.

No, window foiling is not particularly easy to bypass, but remember, it is not necessary that the burglar enter through a window

either. They know that a window that has just been cut is not a pleasant thing to crawl through, and it's not a terribly wise place to be seen crawling. A large hole cut in a window just has "burglary" written all over it, for any chance passer-by. There is also a good chance that the premises are protected by other components (namely preamplifiers) that will pick up on any window activity.

7

Ultrasonic Alarm Detectors

We now move into the study of the next generation of alarms, the area sensors. The first area sensor component we will examine is the ultrasonic alarm. The ultrasonic system consists of a transmitter, which emits a frequency that lies above the human threshold of hearing, and a receiver, that monitors the incoming frequency. The entire system is generally self-contained in one unit, although occasionally one transmitter is used with several receivers.

The sound waves that emanate from the transmitter follow an elliptical (resembling an elongated oval) pattern, and ultimately return to the receiver. If those waves are somehow altered during their elliptical journey, the receiver will know it, and the alarm will sound. Therefore the theory is that if a burglar enters a guarded area, the ultrasonic frequency will be altered by his presence, thus alerting the receiver to an intrusion. The ultrasonic system is very effective, and the range is generally about 40-50 feet.

Although ultrasonic, the frequency that these systems transmit is low, about 20-45 kHz (kiloHertz, or thousand cycles per second). Standard AM radio is between 535 and 1605 kHz. This makes

detection somewhat difficult, but not impossible. The elimination of possible ultrasound users is even easier. People who own pets or who live near a railroad or other source of loud noise are excluded from ultrasonic usage. Pets cause too many false alarms, and the ultrasound may be very irritating to them, since they have a higher sonic perception range. Loud noises create sound waves that interfere with the ultrasonic waves, and create false alarms. Also ultrasound cannot be employed where there is a great deal of movement. Blowing drapes, forced-air heating, falling boxes, Cuckoo clocks, etc. are all causes for false alarms, and generally exclude their owners from the ultrasonic club.

There are several methods of ultrasonic detection. Multi-range bug detectors will reveal the presence of these alarms. Or, with the assistance of an electronics engineer, one could make a device that responds to frequencies between 25 and 45 kHz. Another way is to purchase a multi-band radio or scanner that contains these low frequencies. If the frequencies are scanned slowly, between the aforementioned parameters, an inordinate amount of static and interference should occur when the correct frequency is discovered. Another way, albeit unorthodox, is to take a mouse or hamster near the suspected ultrasonic source, and observe their reactions. Small rodents detest ultrasound, and they usually make every effort to avoid it. (Ultrasound is what is used in those electronic pest-ridders.) Furthermore, there are converters available that bring the inaudible frequencies down to the human's audio perception level. In the presence of ultrasound, these converters will produce a high-pitched hum. Even if prior detection is impossible, professional burglars have observed that transmitters are almost always placed in the corner of a protected room.

Once the sensor is detected and located, what next? How does one penetrate an invisible and inaudible sound barrier, in order to disarm it, without subjecting oneself to immediate detection? If a homeowner caused his ultrasonic detector to blare throughout the neighborhood, after coming home from work every day, he would soon get many complaints from his neighbors. That is why most ultrasonic alarms, and most other alarms as well, have delay switches. They allow the person to enter the house, and disarm the system before the alarm goes

off. It also allows him to arm it, and then leave before it begins monitoring. This type usually has a simple on/off switch on the back, and if a burglar reaches it before the thirty seconds expire, the system doesn't know he isn't the homeowner. This type is usually a desktop model, and usually has an electrical outlet attached to it so that a lamp may be made to come on to scare the burglar. (I've also seen a tape recorder plugged into it which has a recorded message that says "What the hell was that!" when the guarded area is violated.)

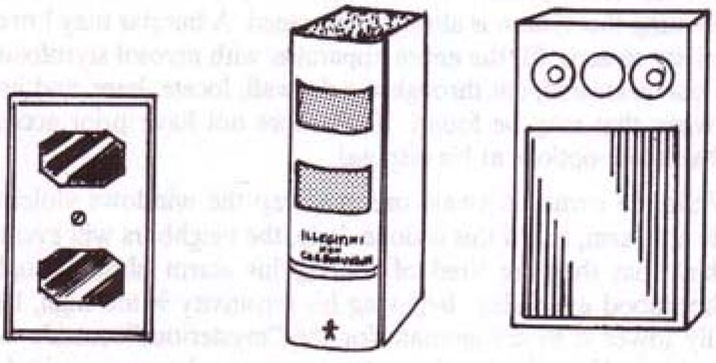


Figure 7-1

Ultrasonic alarms are sometimes disguised as wall outlets, books or stereo speakers.

Because of their simple on/off switch, these are obviously the easiest to bypass, but there are some that are a bit more difficult. They are often disguised as a wall outlet, Hi-Fi speaker, book, or are more conspicuously located on the wall (see Figure 7-1 above). They too have delay mechanisms, but only the book and speaker types have simple on/off switches. The wall and outlet varieties are usually part of a larger, centralized system, and can only be shut off at the control panel. The problem of the book/speaker type then, is simply recognition. The speaker type will be recognized because Hi-Fi's have an even number of speakers, and a third or fifth speaker should stand

out. Also, if a speaker is standing alone, with no accompanying stereo, it is a dead giveaway for thieves. The book type is more difficult to locate when many books are in the room, but it will be a rather thick volume with either two twin circles or squares (transmitter and receiver) on the binding. The name will also be of a generic nature, rather than a "brand name" publisher.

Therefore, the burglar's primary difficulty lies in defeating the outlet and wall-mounted types. There are several techniques that, when used together, enhance the probability of success tremendously. If one has prior access to the protected area while the system is disarmed, success in defeating this system is almost guaranteed. A burglar may lower the sensitivity to zero, fill the entire apparatus with aerosol styrofoam, or, if no one is around, cut through the drywall, locate, bare, and jumper any wires that may be found. If one does not have prior access, he still has a few options at his disposal.

While the owner is away, one may rap the windows violently to create an alarm, and if this is done daily, the neighbors will eventually tell him that they are tired of hearing his alarm blast through the neighborhood every day. Believing his sensitivity is too high, he will usually lower it to compensate for the "mysterious" outside noises. After this is done, the burglar enters wearing a heavy oversized coat, or even a rug, if possible. The more sound-absorbing material a burglar can don, the safer he'll be. The large coat or rug absorbs rather than alters the sound frequencies, and the system's efficiency is compromised considerably. If the walls are covered with rugs, draperies, or tapestries, the effect is multiplied. But absorbing some of the sound is not enough, for the burglar must move super-slow. If the burglar must traverse a monitored area of twenty feet, he may spend at least ten minutes crossing it. The object here is to move so slowly that the frequency remains undisturbed by the burglar's motion. Some ultrasonic units are hidden behind wallpaper or plaster, but this cuts their effectiveness by at least 25%. If the ultrasound units are installed in that manner, they become so unresponsive, the above methods become all the more efficacious.

There is one last remote, yet viable, technique for circumventing this type of component. If one discovers the exact operating frequency of the unit, he could, theoretically at least, get an ultrasonic transducer

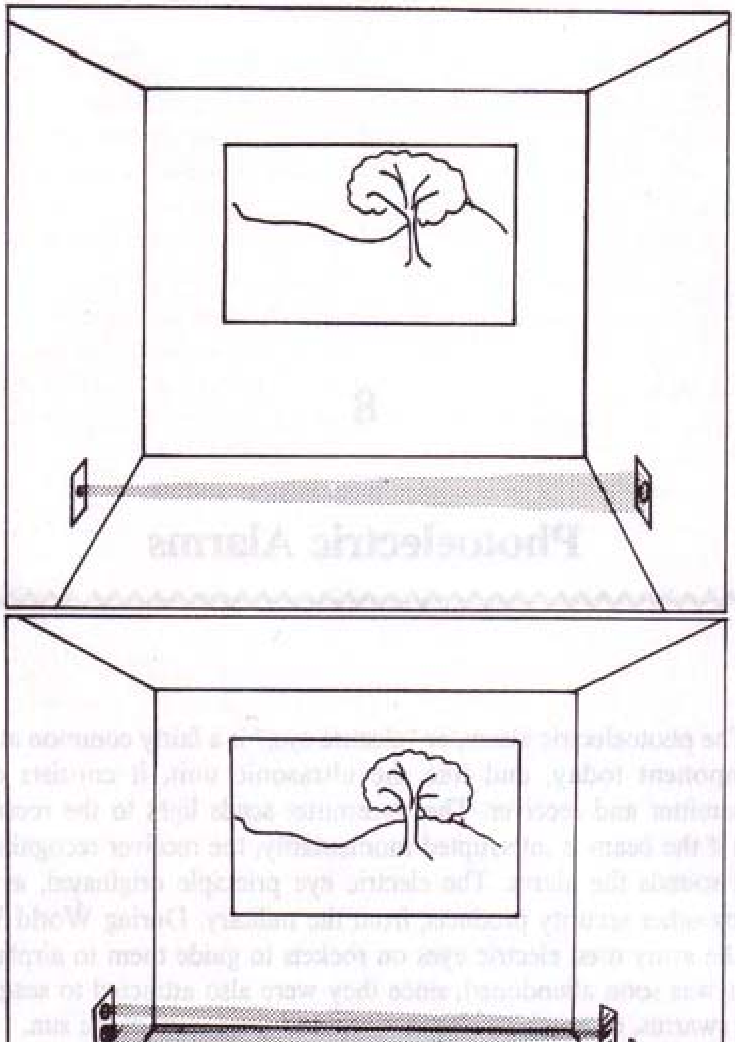
of the same frequency, and stick it in front of the receiving unit. The whole monitored area could be violated because the receiver would constantly be receiving what the transmitter was transmitting. I've never seen this done before, but it is a possibility.

8

Photoelectric Alarms

The photoelectric alarm, or "electric eye," is a fairly common alarm component today, and like the ultrasonic unit, it consists of a transmitter and receiver. The transmitter sends light to the receiver, and if the beam is interrupted momentarily, the receiver recognizes it and sounds the alarm. The electric eye principle originated, as did many other security products, from the military. During World War II, the army used electric eyes on rockets to guide them to airplanes. This was soon abandoned, since they were also attracted to seagulls, bee swarms, or anything else that blocked their view of the sun.

The photoelectric unit may be a transmitter and receiver that oppose each other (see Figure 8-1 on page 44), or the transmitter and receiver may be housed in one unit, while utilizing a reflector at the other end of the room (see Figure 8-2 on page 44). The old type of unit, which is still used in some places, uses ordinary white light. These are simply defeated by shining a flashlight into the receiver, so that a confederate may pass right through the beam. This type is easily detected, especially at night, because the light is plainly visible.



Figures 8-1 and 8-2

Two types of photoelectric alarms.

Even though the newer models use invisible light, they are still terribly easy to bypass. They are placed in front of doors, windows, or in long hallways, in an attempt to catch passerbys. The inherent disadvantage of photoelectric sensors is that they are easily seen. Although sometimes disguised as wall receptacles, they are almost always in plain view, and this fact alone aids in circumvention.

The modern electric eyes use a beam of Ultra-Violet or Infra-Red light. Anyone can buy, from a science supply company, filters that allow them to view UV or IR light. The invisible light is now visible, and may be easily avoided. Trying to shine a beam of UV or IR light into the receiver may work, but the higher-tech models use a pulsed-beam. The receiver will be programmed to the transmitter's frequency, and any deviation will result in an alarm. If one has access to the premises beforehand, he can kick and break the receiver, causing it to malfunction, and causing the owner to shunt that zone before arming the system.

There may be cases where the component uses laser light, instead of Ultra-Violet or Infra-Red. This is easily stepped over, ducked under, or otherwise avoided, provided there is not an entire network of lasers that form an impassable grid. This would only be utilized in a very high-security situation, but since it does occur, burglars have discovered at least two ways in which it may be surmounted. First, a mirror system could be designed that provides a doorway for the burglar. The mirrors must be precisely 45°, and since the apparatus is constructed on the spot, careful planning must go into its design. The viability of the next technique depends greatly on the circumstances involved. If there is a hiding place near the laser-grid, one can walk right through the grid, and then hide. The burglar then releases a bird that he has brought with him. After the alarm sounds, and a guard investigates, he will see the bird near the alarm. He may wonder how it got there, but he will automatically assume that it was the bird that passed through the beams. It should be obvious to the reader that this technique may have applications in other areas of alarm bypassing as well. The laser grid system will certainly not be encountered very often, so a burglar with UV and IR filters may be fairly certain that he is safe from detection by photoelectric alarms.

If the burglar cannot obtain a filter to view Ultra-Violet light, an inexpensive but accurate UV detector is currently available where sunbathing products are sold. Its intended purpose is to warn the sunbather when an inordinate amount of UV energy is detected.

The Infra-Red mentioned above is of the active variety, which means it emits Infra-Red light, and is not to be confused with passive Infra-Red, which is the subject of the next chapter.

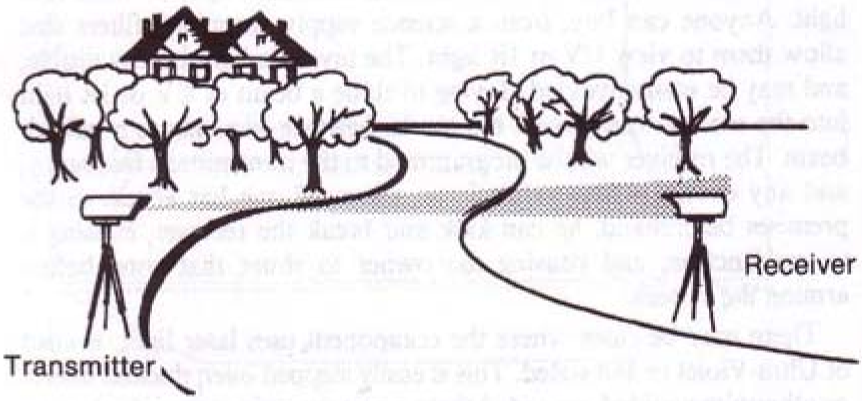


Figure 8-3

An outdoor photoelectric alarm system.

Some companies also use photoelectric sensors out of doors. These devices (see Figure 8-3 above) are placed far apart and are used to monitor the area between them. They are detected and bypassed in the same manner as described above, but they also have an automatic shut-off mechanism that may be of interest. At dawn, dusk, or during an extremely foggy morning, these devices shut themselves off to avoid possible false alarms. This also allows an observant burglar to slip past them at dawn or dusk, or to manufacture "fog" if necessary.

9

Passive Infra-Red Alarms

Passive Infra-Red alarms, or PIR's, are so called because they do not emit Infra-Red energy, but merely detect changes in it. A PIR probes its monitoring area, and if any changes are detected in Infra-Red energy (heat), it sounds an alarm. A PIR records the ambient room temperature so it will notice any sudden change, such as that produced by a human body. Slow temperature changes, such as thermostatically controlled heating systems, will not interfere with the PIR's duties. The PIR is often called a thermal detector, however such heat detectors are used primarily for fire prevention. The PIR is immediately recognizable (see Figure 9-1, page 48), due to its common design and dark-red lens. They are very common in museums, banks, and other places where high-security is desired.

The very fact that a PIR is passive, disallows easy detection. The burglar must rely solely on his observations for the recognition of a PIR system. Due to the nature of a PIR, they are usually placed in a very conspicuous location, such as in the corner of a room. The bad news for the burglar is that PIR's have vandal-proof germanium lenses, are tamper-proof, and cannot be jumpered reliably. Furthermore, the range of the PIR can be 70 feet or more, although a PIR's

probing pattern usually only monitors an area of about 20 feet square (see Figure 9-2 on page 49).

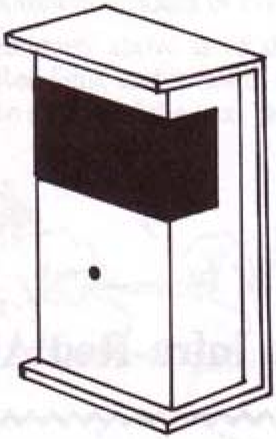


Figure 9-1

A high-security, Passive Infra-Red alarm. The design is easily recognizable.

As reliable as they are, PIR's, as you've probably guessed, are defeatable. Although they are generally undetectable, large-pet owners are immediately eliminated from the list of possible PIR users. With their recent proliferation into the residential market, burglars have learned to anticipate a PIR system. Some are sold over-the-counter, although a great many are professionally installed. Therefore, one means of detection would be to see whether or not the alarm company's window decal was present. In the movies, burglars would mount a transmitting TV camera on a remote controlled car, and drive it around inside the building looking for PIR's. But in real life, the existence of other components would certainly disallow that.

Earlier, I said that PIR's detect rapid changes in temperature. I have walked, albeit slowly, directly up to a PIR, and have not set it off. My movement was so slow that the PIR adjusted to the slight difference in ambient temperature that my body was creating. Even if a PIR system is on a silent alarm (as discussed in Part III), one

immediately knows whether or not he is detected. All modern PIR's have a tiny red LED (light-emitting diode) that lights when the burglar causes the internal switch to close. Although I have walked up to a PIR, it took me four or five times to get it right, therefore just walking slowly is not enough.

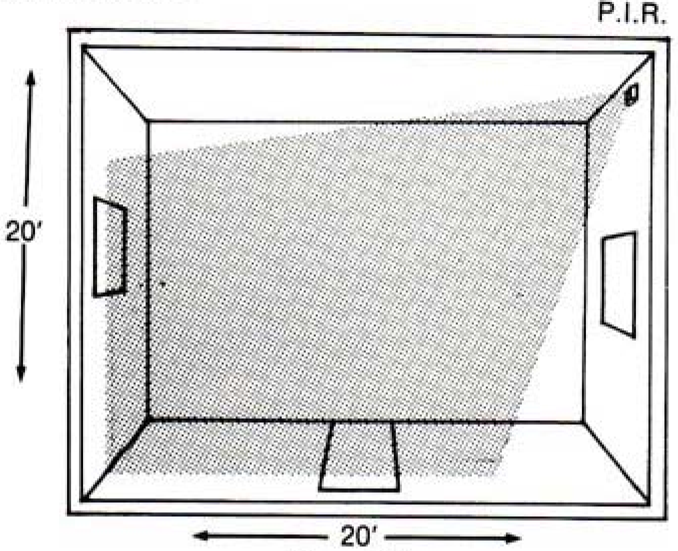


Figure 9-2

Usually located in a corner, a PIR can have a range of 70 feet or more, although it usually monitors an area of 20 feet square.

The greater the distance between room temperature and the temperature of the source of violation, the more efficiently the PIR will work. As the gap between room temperature and the temperature of the violator narrows, the efficiency of the PIR decreases respectively. Therefore, since our bodies maintain a constant temperature of 98.6°, a PIR in a room with a temperature around 100° will never notice you walking through the room. The burglar then wonders: how can I heat and maintain a room or building at near body temperature? One way is to get to the thermostat and turn it on full blast. Another way is to, if possible, make a hole into the room or building, and introduce a large space-heater. It should be at least 350,000 BTU's so that it can produce the required heat. If it blows directly into the path

of the PIR unit, the alarm will sound. The heat must be raised gradually, or the thief defeats his own purpose.

Mylar is a thin, metallic, plastic-like material that has a very interesting characteristic. When worn, it allows very little body heat to escape. If a suit, with a hood, was made of this material, only a small amount of heat would radiate from the burglar, and the chance of detection would be lowered.

If one raised the temperature of the room to 80°-100°, wore a suit of Mylar, and walked very slowly, he would have a very good chance of escaping detection. He may also play the same game described in Chapter 7, so that the owner will reduce the sensitivity. If prior access can be gained to a PIR-protected area, a layer of modelling clay can be spread over the PIR lens to profoundly reduce its sensitivity. The clay may have to be covered with a phony lens to prevent detection. Also, if one gets to the PIR without setting it off, a piece of heavy cardboard can be attached to the front of the lens. A PIR does not probe the heat changes directly above it, below it, or to the immediate sides.

10

Microwave Systems

The Microwave alarm system is another transmitter/receiver motion detector, and is unquestionably the most difficult to successfully bypass. The system emits a beam of ultra-high RF (Radio Frequency) energy, generally 10.525 GHz, and detects intruders by observing any change in that RF energy. Microwave systems are extremely versatile in that one unit may be used to monitor an 80 by 80 room or a 10 by 300 hallway.

The primary disadvantage of a microwave system is that it has a propensity to penetrate the boundaries of the building it is protecting. In other words, microwave energy that is used to guard a business sometimes reaches out into the parking lot, which understandably causes many false alarms.

The detection of microwaves is actually very easy. The frequency they use, 10.525 GHz, is approximately that of police radar. Hence, when you are near a microwave alarm system, a superheterodyne radar detector will sound. The close resemblance between microwaves and radar has prompted people to call these "radar systems," but that is technically inaccurate.

Once detected, quite frankly, there is not much one can do to bypass a microwave alarm in its capacity as a single component. However, they are almost always part of a larger, centralized system that may be defeated. There are some possibilities, however, for the determined burglar, but these depend greatly on the circumstances. For example, microwaves will *not* penetrate metal. If one had prior access to the building being guarded, he could arrange metal objects (filing cabinets, desks, etc.) so that he could reach his destination undetected. Another method that may work would be for the thief to move very slowly. Microwave systems detect movement if it proceeds at more than two inches per second. That is indeed slow, but I suppose one could conceivably move slower. It is very difficult for the alarm owner to know exactly every nook and cranny that his alarm monitors, and even more difficult to adjust it exactly as he wants it. This may allow someone to crawl very low on the floor, or very tight against a wall, and escape detection.

When a burglar knows he is to encounter a microwave system, he usually expects to silence the annunciator (if local), or bypass the entire system (if monitored). As this goes to press, microwave systems are still uncommon for residential use, although they do exist.

11

Traps

The components we'll cover in this chapter have been labeled "traps," because their only asset in burglary detection is their inconspicuousness. If located, they are easily avoided or bypassed, so they are primarily targeted at the amateur and inexperienced. The primary concern for the thief then, is the location and recognition of the trap. Every alarm system is, in a sense, a trap, but what sets the following components apart is the fact that they are so easily avoided if they are simply recognized first.

The traps that a thief may encounter include the proximity switch, the contact mat, plunger switches, lacing wires, glass-break detectors, seismic detectors, and trip wires. Nearly all of these are exclusively used commercially, yet some homeowners have incorporated them into their system as well.

If you've ever seen those lamps and appliances that turn on and off by merely touching them, then you've seen the principle behind the proximity switch. These devices set up a small field that detects the presence of the slight electrical charge in the human body. They are used only on metal objects, such as filing cabinets, and they create a barrier of up to two feet around the object. More often, however, the

sensitivity is set to about 9-10 inches, to decrease the chances of a false alarm.

Proximity switches are easily noticed, because any metal object being monitored will be placed on "insulation blocks." These will be ceramic, concrete, or some similar material that keeps the safe, filing cabinet, desk, etc. ungrounded. One may simply avoid coming into contact with them, or he may resort to other methods if he must get closer, to manipulate a safe, for example. A long, non-conductive gripping device can be constructed (see Figure 11-1) to push, pull, or turn anything that is necessary. It can be made of plastic, glass or anything non-conductive.

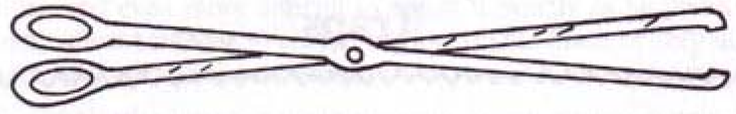


Figure 11-1

Proximity switches can be circumvented by using a long, non-conductive gripping device to manipulate protected objects.

Another trap is the contact mat. They are usually located underneath the carpeting in front of doors and windows, on staircases, and down long hallways. A typical mat consists of opposing contacts that meet and close the circuit when pressure is applied. Contact mats come in standard rolls that are 30″ wide.

They are often difficult to spot, although their tell-tale outline under a rug or carpet is sometimes evident. Burglars avoid walking directly in front of doors and windows, and walk against a wall when traversing a hallway that is over thirty inches wide. When going up stairs, he is especially careful to walk on the edges of the steps, instead of on the flat surfaces that may contain mats.

If he locates a mat that is too large to avoid, he may simply cut one of the wires leading to the rest of the circuit. In most cases, this haphazard method of bypassing would almost certainly sound an

alarm, but the contact mat is unique in that it is a normally open switch. Therefore, if one of the wires is cut, it will remain an open switch, even if walked upon. The ultra-paranoid thief may "walk the walls" using the spiked boots that telephone-pole climbers use, and avoid every contact mat possible.

Plunger switches are sometimes hidden between the door and its frame (see Figure 11-2), so that the opening of the door also opens the switch. They are rarely used when magnetic contact switches are in operation. These switches are also sometimes used behind paintings or under statues. They are simply spring-loaded, and if the pressure is taken off the plunger, the switch opens.

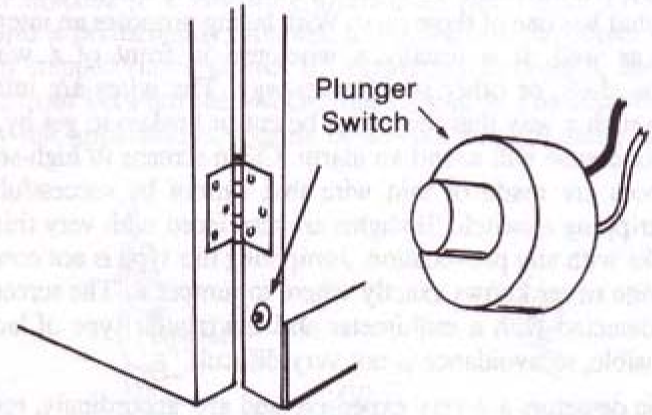


Figure 11-2

Spring-loaded plunger switches activate the alarm when the plunger pops out.

Locating this switch is easy if one has prior access to the location, but very difficult if one doesn't. The most common method is to just assume it is there, although one may keep in mind that professional installers prefer magnetic switches to plunger switches. To bypass it, one may get to the wires from the outside, and jumper them. Or, he may cut through the door, or even tape the plunger switch closed during the day. After the door is opened slightly, one may even reach

in between the door and frame, to keep the switch depressed. For paintings and statues, the best method is to slip a piece of sheet metal between it and the base or wall, so that the switch remains closed after the goods have been lifted.

Two traps that are best avoided are the glass-break detector, and the wire-lacing trap. The glass-break detector is the little round stick-on switch located at the base of windows. Therefore, it is easily seen, but difficult to bypass. One could make a hole in the window with a propane torch, and jumper the wires, but it is so sensitive, it may pick up on this activity. One could also beat the window violently and cause a false alarm every day, so that the owner will eventually become so frustrated he removes it. Otherwise, burglars avoid the window that has one of these on it. Wire lacing proposes an interesting problem as well. It is usually a wire grid in front of a window, ventilation shaft, or other small entry-way. The wires are interconnected in such a way that they must be cut or broken to get by them, and this of course will sound an alarm. Often screens in high-security storm doors are made of thin wire that cannot be successfully cut without tripping a switch. Skylights are also laced with very thin wire that breaks with any provocation. Jumpering this type is not common, because one never knows exactly where to jumper it. The screen type may be detected with a multimeter and the regular type of lacing is plainly visible, so avoidance is not very difficult.

Seismic detectors are very expensive and are, accordingly, reserved for high-security needs. Seismic sensors are completely passive, therefore there are no detectable emissions that signify their presence. The system consists of a main processor, and any number of individual sensors, all of which are buried underground. The information is then sent (by wire or radio) to the control panel.

The seismic sensor is programmed exclusively for the recognition of the distinct "signature" of human footfall. One could traverse a questionable area by hovercraft, but that is hardly practical. Walking very softly or crawling to the target destination will result in a seismic activity that is not recognized by the sensors, therefore the processor will ignore it. The processors are programmed in this manner so that an alarm will not sound every time a squirrel, dog, or bird walks through the area. Seismic detectors are used primarily to guard road-

ways, so thieves who suspect their presence, enter in an unorthodox fashion. Seismic processors are always marked, so that they can be easily located for repairs. If one can find and reach the marker without detection, one can dig to it, and shut it off. Metal detectors are also used to locate the processor or the individual sensors. Incidentally, seismic detectors are almost never used residentially.

The final trap is the simple trip wire. Once used in the jungles of Viet Nam, it has found its way into the security market. These are used to cover vast expanses, such as a factory warehouse or large showroom.

The trip wire itself is a thin string or wire, much like fishing line, and is attached to a switching mechanism (see Figure 11-3) on one end, and is permanently mounted to the wall on the other. When the wire is stepped on or pulled, by attempting to cross it, the block is pulled from between the switch, thus closing it. The trip wire is used in low risk applications, because of the fact that it is easily defeated.

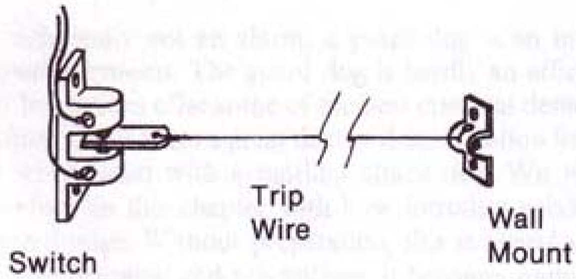


Figure 11-3

A trip wire runs from an alarm circuit to a wall anchor.

Quite simply, trip wires can just be stepped over or otherwise avoided, if they are seen. Noticing them should be easy in daylight, but a bit more difficult in darkened premises. Spray paint that contrasts against the floor can be used to locate them, for a little paint will stick to the wire, but diffuse on the floor. Upon locating these traps, most thieves prefer to cut the line instead of stepping over it,

in case they're forced to leave in a hurry. A strong flashlight shone from the floor may also be used to reveal upcoming trip wires. By the way, trip wires are usually located anywhere from 2″ to 12″ from the floor.

12

The Canine Alarm System

Though technically not an alarm, a guard dog is an integral part of many security systems. The guard dog is hardly an efficient alarm component, but it does offer some of the best criminal deterrence that money can buy. For it takes a great deal of determination for a burglar to proceed when faced with a snarling attack dog. We will be primarily concerned in this chapter with how intruders subdue and/or eliminate guard dogs. Without preparation, this is nearly impossible, but with proper planning and precautions, it becomes quite easy.

There are two types of dogs that a burglar will encounter. The first is the pet, who is kept for personal reasons, rather than burglary protection. The second type is the trained attack dog, who wants nothing more than to eat an intruder alive. Since dogs are extremely territorial in nature, the family pet may sometimes seem as ferocious as the killer dogs, but most often they are more bark than bite. Personally, I would find it very difficult to use the same ruthlessness on a Cocker Spaniel as I would with a trained Doberman, but burglars have no reservations about resorting to these measures to achieve their ends.

Although there are only the two categories of dogs, there are four ways in which they may be encountered. First, and most common,

is the outdoor pet. He is usually chained or tied to his doghouse, and the only problem he presents is his non-stop barking. Another commonly seen type is the indoor pet. He may attack or bark his head off, but usually he will be friendly after a few soft words. The next most common, and also next in line in regards to danger, is the guard dog. He is used in junkyards, car lots, or anywhere else where anyone on the premises would be an intruder. He is generally kept behind a large chain-link fence, to protect the public at large from him. Finally, there is the attack dog, which is specially trained to kill anyone who enters his domain. They often run loose on large estates after dark, and protect it with immense loyalty and vigor. They usually work in teams, and they are often upon the intruder before he knows what is happening.

Depending on the type encountered, there are different methods for dealing with the various dogs. For the first type, the outdoor dog, one may employ a number of silencing techniques. There are the obvious methods such as simply shooting him or giving him poisoned meat, but there are also three more humane methods. Some thieves take two dogs with them, a male and female, when they attempt to make a score. The theory is, and it seems true, that a dog would rather carouse with a member of the opposite sex than worry about any intruders. Also, CAPSHUR is a company that makes tranquilizers and guns that will knock a dog unconscious for a few hours. They sell to the public, if provided with a good excuse. To silence the outdoor dog for a small period of time, one may also use the old mace/stun gun trick. This entails temporarily blinding the dog with mace, or similar irritant, and then using a stun gun to knock him down (and quite often unconscious). The adventurous type may then attempt to muzzle him, but that is not usually necessary. The above methods work for the indoor dog as well, but he may also be simply locked in a closet or bathroom.

The guard dog behind the fence can also be dealt with in a number of ways. A blowgun, which is available from many commercial suppliers, can be used with poison darts to drop the meanest of them. The guard dog is generally trained not to eat anything given to him by strangers, but sometimes he may let a juicy steak get the best of him, and I've also seen a guard dog fed to passivity with Polish sausages. If it were to contain a fast-acting poison, such as tetrodoxin, a simple hot dog would have the same lethality as a rifle slug.

The attack dog wants to kill, and he is very good at his job, but he is ultimately stoppable. He can be shot, blowgunned, or tranquilized, but that takes a good aim, not to mention steady nerves. A large capture net may be carried, and thrown onto an approaching dog, but this quickly becomes futile when one is being approached by more than one. A more effective means of eliminating several dogs at once is to carry a squirt-bottle that has been filled with formaldehyde or hydrocyanic acid (see *Poor Man's James Bond* in the Bibliography). If either is sprayed into the face of the dogs, they will be effectively denied any further attack. The formaldehyde irritates the dog tremendously, but the hydrocyanic acid will instantly kill it. Another interesting method of canine control is the high-frequency Dog Chaser, available from Electronics for Industry, Inc. of Miami. The high-frequency that it emits, creates extreme discomfort for any dog, and the closer he gets, the more painful it becomes. While the Dog Chaser unit in itself may sufficiently insulate one from canine attack, it is generally used only as insurance against the possibility that the burglar's other methods will fail.

13

The Local Alarm Panel

So far, we've only discussed the individual components of the modern alarm system. But in over 90% of all homes that are wired for burglar detection, a central processor or panel controls the system. The panel is sometimes very complicated, or it may be as simple as a key-switch. The purpose of the panel is to provide a means of manipulating the alarm components to suit the owner. For example, at the control panel, one has the ability to shut off the whole system, or just a few of the individual components.

The entire alarm system is comprised of "zones," which are assigned to one or more alarm components. In a five zone system, for example, one zone may be designated for the front door, one for the back door, and three for the windows. Panels may have a capacity of ten or more zones, depending on the system. The purpose of the zone system is two-fold. First, it allows the homeowner to "shunt," or turn off, a particular zone, while leaving all the others intact. If one were to shunt out the zone covering a bedroom window, he could raise it for ventilation, while leaving the rest of the system on guard. Second, zoning lets you designate one door as the specific entry/exit door. The benefits of the entry/exit door will be explained in later chapters.

Below is a drawing of a typical key-operated control panel (see Figure 13-1). Note that it is a very basic panel, and doesn't include such accessories as a panic button or zone control. It does, however, have an entry/exit delay that allows one to enter or leave before the alarm sounds.

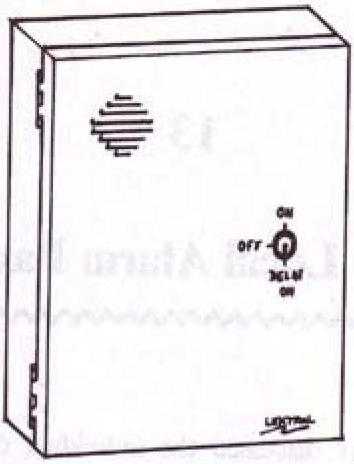


Figure 13-1
A typical key-operated alarm control panel.

The three possible settings for this particular panel are OFF, ON, and DELAY ON. OFF shuts the entire system down, and allows any component, perimeter alarm or motion detector, to be violated with no ill effects. ON arms the system immediately, and is generally used when one is ready for bed. DELAY ON arms the system after about a thirty second delay, which allows one to leave and lock the door. It also allows one to enter and disarm the system before the alarm sounds. Everyone puts their system on DELAY ON (although the wording may be different from panel to panel), when they leave home. Homeowners generally set the delay at thirty seconds, but it may range from fifteen to sixty, depending on the location of the panel. When a system is new, some homeowners set the delay time on fifteen

seconds. But when they walk in one afternoon with two bags of groceries, fumbling around for the alarm key, the time will expire, the alarm will go off, and they will then set the delay for about thirty seconds.

All one needs to bypass this type of panel is the key. But if that isn't possible, there are other alternatives. Now is as good a time as any to discuss the proliferation of locksmithing knowledge. Anyone who has the slightest inclination towards crime has a staggering amount of locksmithing knowledge at his disposal. There are many books on the market that tell you how to pick locks, and even some that show you how to make your own tools. A potential thief may even take an anonymous hands-on course in locksmithing from any of the correspondence schools that offer such training. Not only will they learn to pick all common locks, but the tools are supplied as well. Another benefit of taking the course is that they have the privilege of buying professional lock equipment through legitimate suppliers, and those suppliers are often the only sources of many products. With locksmithing knowledge, one may also be able to make a duplicate key for the alarm, after merely glancing at the original (on the owner's key chain at a gas station, for example). After taking the Foley-Belsaw Institute's locksmithing course, a person can open a lock, without a key, almost as fast as he can with a key. The security of the panel may be increased by using a key-switch of the tubular variety, the type seen most often on vending machines. While somewhat difficult to pick, locksmith suppliers sell a tubular-lock saw that will cut the lock, and allow one to open it, in a matter of seconds. Every variety of control panel, beyond the "El Cheapo" type, has a tamper switch behind the panel door. Any attempt at getting to the inside of the panel will automatically sound an alarm, and there is really not much a thief could do if he were to get there anyway. Therefore, the only way to successfully shut down the panel, is via the key-switch.

Assuming one can pick, or otherwise compromise the lock, the difficulty lies in finding the panel upon entry. It may be on the wall near the door, or hidden in a closet. A bit of night-time reconnaissance will reveal whether or not the person entering has to make a dash towards a closet, or if he remains near the door. Upon entering, most control panels start beeping to remind you that the thirty second delay

has begun. The beeping also leads a burglar right to the panel. The panel must be nearby, to allow the homeowner to get to it in time, so a burglar does a systematic but rapid check of the most logical panel placement. With a good pretext, thieves may even gain prior access to the premises and, with any luck, find it.

The same techniques for location apply to the next type of alarm panel, the key-pad variety. The key-pad offers much more security and often more features than the regular key type. Following is a fairly typical version of the key-pad panel (see Figure 13-2). Note that this panel offers many options, such as a panic switch for emergencies, the ability to "shunt" out certain zones, and the ability to periodically test the system. But aside from the accessories, the only real difference between this and the last type is that you use a key-pad instead of a key. A three or four digit code is entered via the keypad which arms or disarms the system. The same code is used for both arming and disarming, although different people may have different codes.

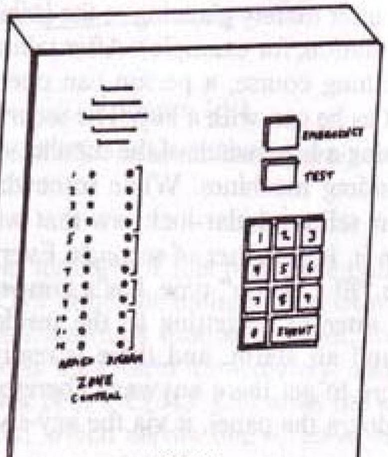


Figure 13-2

A more complicated alarm control panel, operated by a numerical keypad.

No amount of locksmithing knowledge will help a burglar turn this variety off, but there are many other ways to get the disarming code. Depending on the circumstances, it may be possible to get the code through surveillance. Also, the owner's manual for many do-it-yourself burglar alarms has a place in the back to write the alarm code. Many people do write it down and stuff it in a drawer somewhere, and that sometimes offers a dangerous possibility. Burglars have also been known to just go to the panel and start with 001, 002, 003, etc., until they hit the right one. This is time consuming, and the alarm would certainly sound, but when they finally hit the right number, they could call the neighbors and say, "Neighbor, this is Johnson up the street, that was just me. No need to call the cops." Some of the newer models, however, only allow two wrong codes to be entered before temporarily shutting down. After the two minute delay is up, one can enter two more codes, but if they are wrong, the system shuts down for two more minutes. Theoretically, it is still possible to come up with the right code in this manner, but going from 001 to 999 would take at least 16 hours, and going from 0001 to 9999 would take days.

A very reliable way to get the code, is the UV ink method. Moments before the home or business owner arrives, a large quantity of Ultra-Violet ink (available from scientific suppliers) is distributed on the door knob. When he goes to disarm the system, the residual ink on his hand will remain to some degree on the keypad, and this can later be seen under an Ultra-Violet lamp. It would then be a very simple matter to deduce the possible combinations of the code. This technique always works for left-handed homeowners, since they use their left hand to both turn the door knob, and disarm the system. But right-handed people are a bit different. The right-handed person sometimes turns a door knob with his left hand, then punches the disarming code with his right. Burglars have conquered this problem by sprinkling, with Ultra-Violet ink, a package that he has to pick up with his right hand. The package may be in the form of a briefcase, box, trashbag, or anything, but is laid in such a manner, that a person would be obliged to use his right hand to pick it up.

One last technique used for discovering the code works only when one code governs the entire system. The control panel is dusted with a detective's fingerprint kit, and the latent prints should be revealed on the numbers that make up the code. If two or more codes are used in a house or business, the dusting will reveal every digit of every code used, and therefore this technique would probably be futile.

14

Miscellaneous Local Alarm Information

Before we begin the study of monitored alarm systems, there are a few loose ends that need tying. Let me reiterate that there are three major ways to defeat the simple local alarm. These include silencing the annunciator, bypassing the individual component, and shutting down the whole system. Of course, a combination of all three is even more effective, as professionals know that when bypassing alarms, there is no such thing as overkill.

The first two weeks after a new alarm system is installed, the home or business owner will accidently set it off many times. During this period, the neighbors or surrounding businessmen will dismiss the alarm signals as false alarms. Obviously, this is a wonderful time for the burglar to strike. (Of course, the best time is before they even install the alarm system.)

Burglars also send away for the literature that the alarm companies distribute. The literature often gives technical information and usually has photographs of the different alarm panels. Under some circumstances, this may aid in defeating the control panel. If the homeowner displays a "This Property Protected by XYZ Alarms"

sticker, the XYZ Co. will be pumped for all the information they can deliver.

Another topic that belongs in the miscellaneous category is the proliferation of the "Dead Man Trap." While expressly illegal, some do-it-yourself types set up a contraption that is meant to maim or kill an intruder, rather than catch him. This may be a loaded gun aimed at a window, a jewelry box that blows up in the face of anyone who opens it, or a safe that is wired to deliver 50,000 volts to anyone who touches it. The homeowner who installs such a system had better be prepared to lose more in court than from a burglary. There are many cases on record where an injured burglar actually sued and recovered thousands of dollars from the homeowner he was burglarizing. Aside from being sued by would-be burglars, there are just too many dangers involved to consider this type of installation as actual protection.

Finally, it may have occurred to the reader that when one attempts to bypass component A, there is a very good chance that component B will detect that activity. For example, if a thief attempts to bypass a magnetic switch by cutting a hole in the door with a chainsaw, it is likely that an ultrasonic detector will pick up this disturbance, and create an alarm. Or, if one attempts to avoid window foil by cutting a hole in the window, the glass may fall onto a contact mat, and sound the alarm anyway. That is why most professionals only bypass the components necessary to reach the control panel, where they attempt to shut off the entire system. This allows them to operate on the control panel, without having to worry about any time delay mechanism.

PART III

Monitored Alarm Bypassing

In Part Three, we will discuss the variety of systems that are monitored by a central station. Rather than announcing an intrusion (via bell, siren, etc.), this type of system silently sends a signal to the alarm company where people are monitoring for intrusions. This type of system, therefore, is often referred to as a "silent alarm." Although one can obtain his objective by bypassing the individual components of a local alarm system, when bypassing this type, one must shut off the entire system to be successful. The employees of the central station are led to believe that the alarm is being shut off by authorized personnel. Therefore, burglars are not only aware of the techniques of bypassing this system, but also of the psychological maneuvers that are necessary as well.

15

The Central Station

A few years ago, rich homeowners, business owners, and other potential targets for burglary, had alarm systems that were tied in directly to the local police station. As the use of burglar alarms increased, the police department began turning down more and more requests to be "hooked-up." As a result, there became a demand for central stations, or companies whose specialty it was to simply monitor burglar alarms. Most police departments will still allow banks and large jewelry stores a direct link to the police station, but as a rule, homeowners are excluded. As the demand for security has risen, many guard agencies and burglar alarm installers have begun to offer centralized monitoring as an option for their clients.

When a silent alarm is installed, it is connected by a dedicated telephone line to the central station. In the event of an intrusion, the control panel on the premises being monitored calls up the central station and gives an electronic message to the answering computer. It tells the computer exactly which switch or sensor has been violated, and the computer then tells the operator what has happened. For example, if a burglar entered through a broken window, the panel would call the computer up, and tell it that zone 4, a first floor window, has been

broken. The operator would then see on his computer screen that Acct. #1234, the Johnson residence, has had zone 4, the window foiling on the living room window, violated. As the thief progressed through the house, the panel would call the computer for every sensor that was violated. The operator may then receive 1234-17, meaning that zone 17, a Passive Infra-Red detector in the master bedroom, has detected someone. The operator would then be fairly sure someone was in the house, so he would have three options. He may just send his company's armed guards to the scene, call 911 and dispatch the police, or he may send both the police and the guards. (See Chapter 19.)

When an authorized person enters through the designated entry/exit door, he goes directly to the control panel. Using a key, or his push-button code, he shuts the system off. If he enters at a strange hour, he must call the central station and give them his password or code phrase. And so, since the system was properly disarmed, the central station operator then pays no more attention to that particular account for the rest of the night. Because of the time delay, the owner is able to shut it off before the panel has time to call up the central station's computer. This, coupled with the fact that the owner calls the central station to give them his code, supposedly guarantees against foul play. The premise here is that even if a burglar can get to the panel, and shut it off, he will not know the code word. I suppose the people who think that have never heard of bugs or telephone taps, not to mention laser surveillance devices, parabolic and directional microphones, or the "Oops, I forgot my coat last night" (which contained a voice-operated tape recorder) trick. The entry/exit door is another safeguard against illegal entry. It is designated by the owner at the time of installation, to be the ONLY method of entrance when the alarm is armed. That doesn't mean that the owner always obeys this, but it causes the central station operator to be a bit more suspicious if someone shuts off an alarm, but does not enter through it. Since the best way to bypass a monitored alarm is to appear to be authorized to do so, a burglar usually does some surveillance to determine the entry/exit door.

A central station has an immense amount of control over the security of its city. The central station keeps blueprints (containing the

alarm design) of clients' buildings, the master codes and codewords for all alarms, and it sometimes even keeps a copy of their keys. It also knows when their clients are out of town, and how long they will be gone. Ideally, a central station would be an impenetrable fortress, and its employees would all be unquestionably trustworthy, however, in most cases, neither is true. Chapter 21, on Guerrilla Tactics, will show how these weaknesses are exploited.

It would greatly benefit a thief if he knew whether or not a system was monitored, and if so, by whom. Ordinarily, a security company puts its sticker on the doors and windows of a monitored house. The thief could look through the local Yellow Pages, to determine if the security company was legitimate, and also to determine how fast the guards could arrive. A common way that is used to determine if a house is indeed monitored is to throw a rock through a window. If a bell sounds, it is more than likely local, if there is no sound, but cops arrive moments later, it is monitored. After a house or business has been determined to have a monitored system, there are several ways to determine the company that monitors it. Let's say that the proposed target is Movie Rental at 716 Broadway Street. One could call every alarm company in the Yellow Pages, and say, "This is the police department, do you monitor Movie Rental on Broadway?" Usually, an answer will be given, but a reason for wanting to know should be prepared. Presumably, one company will eventually say that they do indeed monitor Movie Rental on Broadway. Another way to find out who monitors the alarm is to strike up a conversation with the proposed victim, and ask him to recommend a security company. A less risky way is to throw a rock through a window containing foil, or otherwise break an alarm component, and see who comes out to fix it. The name of the company is usually written on the service truck for advertisement, but if not, the license plate is run through the DMV computer. In rural or suburban areas, one could also check the homeowner's mail for the alarm company's bill.

An alarm company not only monitors for intrusions, but also for tampering and sabotage. Cutting the telephone lines, the power lines, or tampering with the control panel, will bring the cops just as fast as breaking down the door. Although leaving the telephone off the hook will prevent the alarm company from contacting the house, it

will not keep the control panel from contacting the company's computer, because it features a "line seizure" mechanism. That means that no matter what happens, an alarm signal will still get through to the central station's computer.

16

Preamplified Microphones

One individual component was not discussed in Part II, because it distinctly belongs in the section on monitored alarms. This component is the preamplified microphone, or preamp, as it is called. It is usually a small black box that sits in a centralized location, and listens for anything out of the ordinary. Many companies, notably Sonitrol Security, utilize preamps in addition to regular components. When the system is armed, the preamplifier sends sounds (via telephone wires) to the central station. The preamp can pick up the slightest noise, so that the tell-tale sounds of a burglary betray the burglar even if the other components do not. The preamp does not know the difference between the sounds of burglary and everyday noises, so it also sends barking dogs, sirens, telephone rings, and various other "harmless" noises into the ears of the central station operator.

Although they are sometimes detected with high-quality bug detectors, it is often quite difficult to ascertain whether or not they are being used. However, if a thief knows (or thinks) a preamplifier is being used, they are quite easily overcome. If, prior to execution, one calls the residence or business, the ringing will continue until the burglar arrives. If the burglar is very quiet, the ringing will mask the

noise that he is making, and the listener will be none the wiser. Similarly, a tape recording of a siren or barking dog is often used to create the same effect.

Some security supply companies sell a sound generator or jamming device that nullifies bugs and other microphones, but the interference that this creates may arouse undue suspicion, so it may not be practical for all circumstances. One method that is practical, however, is the use of a CB linear. If a CB radio that is connected to a powerful linear (over 250 watts) is used near a preamplifier, the only thing that the operator at the central station will hear is the CB conversation. You may think that this would immediately arouse the suspicion of the operator, but actually it probably won't, because it happens all the time. Everytime a trucker with a powerful CB radio passes by a home or business with a preamp this phenomenon occurs.

Since preamplified microphones also capture the sound of an authorized entry, the code is usually just given aloud upon entering, so the operator can shut off his system. This code, then, is extremely easy to surreptitiously obtain.

17

The Monitored Control Panel

The monitored control panel doesn't differ greatly from the local control panel. It is usually key operated or push-button controlled, and the same techniques of locksmithing and procuring the alarm codes apply to it. It does, however, have a few extra features that merit it an individual chapter.

A hold-up switch or panic button is usually tied into a monitored alarm system. Sometimes several are scattered throughout a home or business, and if any are pressed, it immediately sends an emergency signal to the central station. The central station is generally ordered not to call the premises on a hold-up alarm, but rather to call the police immediately. There is a hold-up alarm in every bank, convenience store, and liquor store in the country, although they are usually disguised. Some are foot-pedals, while others are a metal clip device with a removable banknote between the contacts. A residential panic button works in the same manner, although it is rarely disguised. Many systems allow a wireless panic button to be placed by the bed, so that one can push it without going to the panel.

Another feature of the monitored alarm panel is the duress code. A duress code disarms the system, but at the same time sends a distress

signal to the central station. If a thief breaks into a house while someone is home, he may threaten to kill the homeowner if he doesn't give him the disarming code. The code is given to the thief, and it in fact does shut the system off. What the burglar doesn't realize is that in five minutes the home will be surrounded with cops. This would work almost every time, if the security industry had not standardized their duress procedure. Every company that I know of advises its clients to add 1 to their regular code to send a distress signal. For example, if your regular code is 1234, and a burglar demanded the code from you, you would give him 1235. It would disarm the system, but also notify the central station that there is trouble. The problem here, is that an intelligent burglar could just subtract 1 from whatever code you gave him, and try it first. If the system disarms after subtracting 1, then the code the homeowner gave was the trick, or duress code. If it does not disarm after subtracting 1, the homeowner gave him the correct code. Either way, the burglar escapes the trap that was set for him.

18

Pavlov's Dogs Effect

In the nineteenth century, Ivan Pavlov conducted an interesting psychological experiment. He rang a bell every day before feeding his dogs, and eventually the mere ringing of the bell caused the dogs to salivate. This was the first scientific recognition of what is known today as a conditioned response. What has this got to do with alarm bypassing? Not much, but the same conditioned responses have their use for the crafty burglar.

Because some alarm components are very sensitive, they are often prone to false alarms, and, due to mechanical failure, some components are more prone than others. In addition to this, there are recurring incidents, such as a loud truck that drives by a certain spot every evening, or a manager who always takes too much time to get to the panel, or many other events, that send an alarm to the station every day at the same time.

Obviously, if this goes on for any length of time, the operator will begin to expect it, and then to ignore it. I remember an alarm that belonged to a storage company that would come in almost every night. The first few times, we sent the police to investigate it, but soon we began sending only our armed guards. Although we repeatedly

sent servicemen to try and fix it, we eventually began to accept it, and then ignore it. You may have guessed that when they were burglarized a month later, our company was unable to explain to the owners why we did not respond to the alarm.

It was a textbook case of the Pavlov's Dogs effect. The secret of this technique is to make a single component ring into the central station every night or so. Eventually, there will be so much laxity towards that individual account, it can be violated, and the police will probably never even be notified. While the ideal situation calls for violating a single component, burglars sometimes find it necessary to violate more than one. This game, however, is not played as long as the single component game, because a much more in-depth investigation will be made by the alarm repairmen. It is also possible to use the Pavlov's Dogs effect on local alarms, by getting the neighbors and police tired of responding to false alarms, but it is more effectively used when the alarms are monitored.

There is another advantage for the burglar if he causes a large number of false alarms at a particular location. With the increasing number of false alarms, many police man-hours are being wasted just responding to them. This has prompted many cities to adopt an alarm ordinance. The ordinance only allows a home or business owner a certain number of false alarms during a thirty day period, and if that limit is exceeded, their alarm license will be temporarily revoked. If someone's license is indeed revoked, an alarm cannot be reported to the police during the punitory period. Obviously, if an account is only one alarm away from violating the ordinance, the central station operator is going to be quite apprehensive about notifying the police the next time an alarm comes in. The operator will certainly not call 911 if there is any doubt as to whether or not there is an actual intrusion at the location. You may rest assured that the professional burglar can quote the alarm ordinances of the cities in which he operates.

19

Police And Guard Responses

Although a burglar may proceed with caution, defeat every alarm component in sight, and shut off the whole alarm panel, there is still a chance that he may make a mistake. If the mistake is insignificant, no one ever knows about it, and his mission comes off smoothly, but if the mistake raises the suspicion of the central station operator, it may result in the dispatch of guards or police to the premises. The professional burglar recognizes this possibility, and often takes steps to minimize the risks and dangers of getting caught. With enough planning, not only will his mission be accomplished, but the burglar will also probably escape.

If a burglar creates a silent alarm, or otherwise arouses the suspicion of the operator, the police, guards or both, may be sent. If the alarm company has its own mobile guards, it will dispatch them to the scene via radio. This radio frequency is easily discovered by networking with scanner enthusiasts, or by writing the FCC. Once the frequency is procured, the burglar can listen to and follow every move of the guards. If the guards are headquartered at the central station, a confederate can keep the place under surveillance, and watch the guards' activities. If they suddenly go to their vehicles, and proceed toward

the place being burglarized, the confidant will notify the burglar by walkie-talkie. If the potential take is large enough, burglars may even have several cars strategically placed along all possible routes that guards and police must use to arrive at the scene. If they observe anything relevant, they will notify the burglar. They may also bug the central station (see Chapter 21 on Guerrilla Tactics) to determine whether or not the guards will be sent.

If a company does not have guards, or if they feel the police would be better equipped to handle the situation, they may just call 911. The operator will talk to the police department's dispatcher, and tell him that he has an "alarm drop" at such-and-such address. The police dispatcher will then notify a nearby unit, by radio, that he received a call from XYZ Security, and that he should go check it out. The burglar, who also has a scanner preset to the police frequency, has also been notified, and is mysteriously gone when the police arrive. The frequencies of local police departments are easily obtained from fellow scanner listeners, or from the Radio Shack frequency guidebooks.

While the above techniques will work in most cases, there may be times when a guard or policeman arrives, without the burglar knowing about it. If this occurs, it is usually during a routine neighborhood check, or when a policeman is stopped and diverted to the scene by a suspicious neighbor. This, however, is so incredibly rare that the chances of being caught in this manner are almost nil.

If a burglar thinks that he has a chance of getting caught, he may obtain authentic or counterfeit credentials and documents that provide a plausible excuse for his being there. Willie Sutton, the famous bankrobber, even went so far as to make a complete, but phony, police uniform to throw everyone off of his trail. This technique would obviously have its uses in housebreaking as well.

Professional burglars also know better than to hide on the premises to avoid capture. After the guards and police arrive, and verify an actual point of entry (POE), the police department will bring out its K9 unit to "sniff out" the place. Anyone hiding in the home or business will be found in a matter of minutes. It seems that thieves would rather take their chances as a moving target than to be a sitting duck by hiding under a bed. If one enters in a conventional manner, such as through the front door, he usually takes care to lock it behind

him to give the appearance that nothing has been disturbed. If a guard or policeman arrives on the scene and doesn't notice anything suspicious, and doesn't see anyone inside, he will usually proceed no further, and write it off as a mechanical failure. Obviously, if a thief uses a crowbar to open a door or window, no one will think it was merely a false alarm. Closing and locking the door behind him also minimizes the risk of being caught during a routine door check, which is quite common in some cities.

Finally, it should be known that professional burglars are acutely aware that most guards are either 18 and just out of high school, or over 50 and extremely out of shape. Either way, they are poorly paid and extremely indifferent to their company and clients. They have no inherent loyalty toward their employers, and this generally provides an incredible opportunity for the resourceful burglar. It is obvious that five thousand dollars in the hand of a $3.50 per hour security guard will sometimes make him look the other way for an hour or so.

20

Television Monitors And Auto-Dialers

Closed Circuit Television (CCTV) cameras are used around the world to keep vigil over areas that are potential scenes of criminal activity. In many cases, a guard keeps watch over several monitors, or the cameras are connected to VCRs so that they may be reviewed later. Cameras may also be connected to motion detectors, so that if anything is detected within the camera's field of view, it will scan for the intruder. The motion detector system is used when a guard has to monitor such a large number of cameras, it would be difficult to watch them all simultaneously. CCTVs are frequently seen in hotel lobbies, at bank teller windows, and other areas where the very presence of the camera deters crime. In reality, however, cameras do very little to guard against a professional burglary.

In the movies and on television, there is a variety of methods used to defeat the lowly CCTV camera. Some thieves spray shaving cream into or tape cardboard over the lens. *MacGyver* simply places a mirror in front of the camera, and the *Mission: Impossible* team taps into the coaxial cable, and delivers a phony picture to the Third World guard. Fortunately, or unfortunately, depending on your viewpoint, it is never quite that simple. CCTV cameras have the uncanny ability to

penetrate seemingly opaque objects, therefore the shaving cream/cardboard method would probably not work. A mirror placed in front of a lens would be a definite giveaway for an observant guard that something was askew. Finally, the "tapping into the coax" trick would involve so many trial and error adjustments that no one could get it right the first time, let alone convince a guard that nothing out of the ordinary had happened.

The primary characteristic of a CCTV that allows for easy bypass is its outstanding visibility. This fact alone allows an observant thief to watch the scanning rate of the camera, and do his "work" during the periods when the camera is looking the other way. There are often attempts made to disguise a CCTV, but any suspicious box aimed at a sensitive area is automatically assumed to be a surveillance camera. Sometimes video cameras or slow-speed Super-8mm cameras are hidden in liquor stores and gas stations, and are turned on by a hidden switch or foot pedal. These certainly won't deter crime, since the amateur criminal doesn't know they're there, nor will they apprehend many professional criminals, since a pro would obviously wear a mask or disguise during such an operation.

There are two more video surveillance devices that are practically useless for criminal detection. First is the phony TV camera used in some stores to fool people into believing that their every move is being watched. This does deter shoplifting among amateurs, but professionals know them for what they really are. Some of these fake cameras can even scan and they may appear to be completely authentic, but a professional thief is more aware of current security products than the store owner, and has undoubtedly studied the brochure on these phony cameras as well. The second device that I feel is virtually useless for criminal detection is the still-frame transmitting camera. This type takes a still photo of an area such as a parking lot, and transmits a picture, through the telephone lines, to a monitor that is connected to the same phone line. The monitor may be anywhere in the world, provided there is telephone service to that area. But the monitor only receives a new image every minute or so, so that anything that transpires in the minute between one picture and the next, will go unnoticed. Also, if the telephone lines to and from the monitor are cut, there is no more surveillance until a repair crew can get to the sight to mend them. So much for security.

There are two more techniques for defeating the surveillance camera, and their use depends on the manner in which it is monitored. If the camera is connected to a video-tape recorder, the lens may simply be covered with a glob of modelling clay, or any other moldable opaque substance. If this is done, no activity in the monitored area will be captured on film. If the camera is being monitored in real time by a guard or policeman, an FM oscillator (the type sold in novelty catalogs to interfere with TV and radio broadcasts) can be altered to produce several hundred watts. If this device is brought anywhere near a TV monitor, the picture will be reduced to snow and static.

The auto-dialer is equally worthless in preventing professional burglary. The auto-dialer is a device that calls a central station or police department on the telephone and delivers a short pre-recorded message that there is a burglary in progress. There may also be other numbers listed, such as those of friends and neighbors, in case some of the other calls did not get through. Modern auto-dialers have a line-seizing mechanism that disallows jamming the line, by calling the residence prior to the housebreaking, for example. They are usually hidden and housed in a locked box for added protection, but even with these safeguards, the value of the auto-dialer as a security device, is practically nil.

If the alarm that is connected to the dialer cannot be bypassed, the telephone lines cannot be cut, and the lock on the housing cannot be picked, there are still several more ways to defeat this system. Since auto-dialers are silent to the homeowner as well as the burglar, they are party to many false alarms. This fact has prompted many cities to ban the use of auto-dialers, since so many police man-hours have been wasted responding to them. In the cities that do allow them, the homeowners have been advised to install abort switches in the home. At least one abort switch, which shuts the dialer off immediately, will be placed near the dialer, in the master bedroom, or near the control panel. Of course, some dialers have a simple on/off switch on them, and they must rely on concealment alone to beat the burglar. However in the average home, there are not too many places that one can adequately hide something as large as an auto-dialer.

Perhaps the quickest method to defeat the auto-dialer is to simply erase the tape. Since the message is recorded on magnetic tape, an electromagnetic bulk eraser will leave the tape completely blank. This can also be done with a regular magnet, provided it is powerful enough. The fact that this can be done without removing or opening the protective cover, makes it a particularly dangerous possibility. If the tape is subjected to a powerful magnet, even if the call goes through to the police, they will hear nothing but a constant hissing noise.

21

Guerrilla Tactics

There may be cases when the burglar cannot bypass or avoid an alarm system, therefore he may have to resort to guerrilla tactics to accomplish his goal. When I say guerrilla, I mean a method of attack that is so unorthodox, no one could possibly expect it. Although the term guerrilla generally conjures up images of brutality and ruthlessness, the term here means simply that the tactics that are employed are so unique, they generally leave everyone, including the police, temporarily stunned. Guerrilla tactics are usually only aimed at central station employees, or the central station itself, but they may also be used against the police department, if the need arises.

Ideally, the central station would be a veritable fortress. Unfortunately, they are most often a rented building in a bad neighborhood, or a leased unit in an office complex. The only security system that protects the central station is usually a TV camera at the front door, and a simple local alarm. Sometimes the sales office, where one must go to inquire about having an alarm installed, is adjacent to, or part of, a central monitoring station. There would obviously be much information to be gleaned, if one were to plant a bugging device or tape recorder near the central station, during his alarm inquiry.

Similarly, an Infra-Red laser surveillance device could be shone on any window to pick up the juicy central station gossip. If prior access is impossible, the telephone wires may be cut at the meter base, although most central stations have standby generators, in case of a power failure.

The employees of a central station also offer the burglar some unique possibilities. The poorly paid central station operator is extremely susceptible to bribery, and he may be induced into carrying a disguised bugging device, if he is unaware of what it is. A bug disguised as an engraved ink pen, for example, may be given to him as a gift, in hopes that he will carry it around with him, and especially to work. Other employees of the agency, such as installers, can also be bribed or induced into installing a system that would be very easy to defeat. The installer may also know, and be willing to sell, the master code that controls someone's system. The patrol cars that the armed guards use when responding to an alarm drop may also be made useless, by slashing the tires, placing caltrops under the tires, or filling the roads near the proposed target with tacks, broken glass, and caltrops. The engine, gas tank, and transmission, may also fall victim to various methods of incapacitation. In smaller cities, where comparatively few alarms are monitored, only one or two employees work the Midnight to 8 A.M. shift. During this period, the central station could be stormed, and the employees detained. Also, poisonous or anesthetic gas could be introduced into the central station, so that the operators would be disabled. Operators could also be extorted for sensitive information, if one could find the proper motivation, such as threats, money, blackmail, etc. Police departments are less vulnerable to guerrilla tactics, but they are certainly not invulnerable to them. At a small town police department, squad cars could easily be incapacitated in the same manner as described previously. Although less likely to be bribed, policemen can sometimes be pressured into taking their good-natured time when responding to an alarm drop. The burglar could also place several obstacles along the route the policeman would take, so that he would be delayed in getting to the scene.

The station itself can also fall victim to sabotage. A burglar could bug a police station and learn a great deal, such as information on potential targets or police schedules. A confederate may also listen to

the police station conversation to discover whether or not an alarm call has been made. And since the alarm company must call the police department to report the alarm, the incoming telephone lines may be tapped into or cut. Since the police department has a limited number of 911 and routine lines, it is also possible for several recruits of an intelligent burglar to flood the 911 lines, so that the central station cannot get through to notify them of an alarm. This is easily accomplished in the smaller police departments, since they usually have no more than five incoming lines. The telephone also offers the possibility of using a decoy. This involves calling the police station to tell them of an awful wreck, break-in, rape-in-progress, etc., so that the policemen will be dispatched to that area, and the burglar can work (on the opposite side of town) unhindered. One possibility in defeating a large police department, where patrolling policemen are dispatched to alarm drops by radio, would be to actually override the police frequency with another transmitter. This would be extremely expensive to do, therefore the stakes would have to be very high.

PART IV:

Miscellaneous

In the fourth and final section, we will examine the phony burglar alarm system, and how it is so easily recognized. No longer are these just the product of the do-it-yourselfer, but are also being produced commercially at an ever-increasing rate. There seems to be an almost insatiable demand for these devices that supposedly scare criminals away. You will find, however, that they sometimes do more harm than good. We will also cover some random topics that, although related to alarm bypassing, could not be appropriately placed in any of the preceding chapters. Finally, we will cover the state-of-the-art security systems being installed today, and the future alarm systems that will be installed tomorrow.

22

Phony Alarms

Surprisingly, it is generally believed that the burglar alarm's primary task is deterring, not catching criminals. While it is true that many thieves will not enter a dwelling that they believe is guarded, perhaps the most dangerous type of criminals will probably disregard it. The drug-crazed kid who needs some quick cash for his next fix will probably not pay any attention to an alarm. Nor will a mentally deranged criminal, who probably doesn't even care if anyone is home or not. Furthermore, we've seen that the professional burglar has no apprehensions about entering a building that is on an authentic alarm system, much less a phony one. The professional will not be impressed by the flashing lights and warning stickers, but rather will recognize it immediately as a complete scam.

It doesn't take a great deal of detective work to determine whether or not an alarm system is authentic. On page 98 is a typical phony alarm panel (see Figure 22-1). It is generally installed in a conspicuous location, such as near the front door, and it usually has a red flashing light. This presumably warns that the system is armed, and is currently monitoring the premises. Rarely, however, are actual control panels mounted out of doors, to be subjected to vandalism, and never are

they mounted with simple Phillips-head screws. The panel below is actually just a key operated switch that will simply turn the red light on and off. Since the homeowner knows his system is spurious, he will occasionally forget to disarm his system before entering his home, as surveillance will prove.

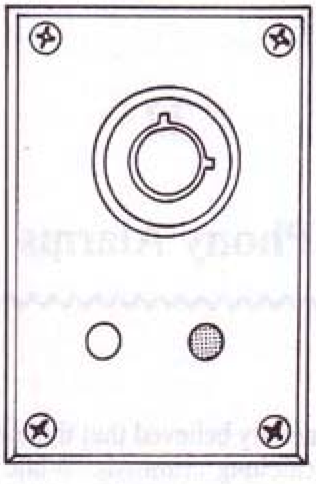


Figure 22-1

A phony alarm control panel is easy to spot.

Stickers that warn of alarm systems abound in electronics and novelty stores. Authentic alarm stickers display the manufacturing company's name and/or logo, but the generic "This Property Protected By Electronic Alarm System" stickers are painfully obvious for the initiated (see Figure 22-2 on page 99). A professional burglar, when seeing a fake alarm system with phony stickers, may become even more intrigued with what you are trying to protect than he would if there were no alarm at all.

While some security books say that a few flashing lights and an impressive looking key-switch will deter thieves, I believe the money would be better spent on a real alarm. Even though a professional can defeat it, a real alarm has the capability of catching a thief, rather than just the hope of scaring him away.



Figure 22-2

Phony alarm stickers may attract more criminals than they deter.

23

Related Subjects

The purpose of this chapter is to examine some of the more esoteric subjects related to alarm bypassing. Basically, there are four random, but important thoughts that need elaboration here. I decided to pile them into one chapter, rather than spread them through the book where they would normally belong, for fear that their importance may have been inadvertently missed.

First, one should know the various steps that some professional burglars take to improve their chances of success on a particular mission. Before, during, and after a burglary, there are many techniques that may be employed that virtually guarantee that the heist will come off smoothly. Some techniques, such as wearing gloves to avoid fingerprints, and wearing a mask to avoid being recognized, are obvious. Other techniques, such as planting "artificial" clues, are not so obvious. The nemesis of any criminal is a betraying clue that links him to his crime. Often this betraying clue can take the form of a distinctive modus operandi. Burglars who maintain the same procedure of housebreaking for any length of time may find it necessary to change their B and E techniques. One of the hallmarks of a true professional is his ability to look incompetently amateur. Broken windows, smash-

ed doors, crowbar pryings, all reek of amateurdom, and effectively throw the ensuing investigation off the scent. The only drawback of appearing to be a rank amateur is that one may obtain the same results (such as setting off an otherwise easily defeatable alarm) that an amateur would.

Second, when an alarm is monitored by a central station, the operator receives a signal for every alarm component violated. He also receives a signal for every component that has been restored. This means that when a door, that has been opened, is suddenly closed, the operator receives a signal that corresponds to the restoral of that particular zone. This may seem irrelevant, but if an operator receives a violation, and then a restoral, he knows the door has been opened and then closed. If, however, he receives only a violation, with no restoral, he may be a bit more inclined to believe that the violation is a false alarm, since a person would obviously close a door behind him.

A constant source of debate among my colleagues and I is the question of the best time for a burglary. Of course, this depends tremendously on the circumstances, but there are times that are more conducive to success than others. For example, during an electrical storm, a central station may receive dozens of false alarms. If the electrical storm occurs on a Saturday afternoon, the endless comings and goings of store owners, coupled with the false alarms from the storm, keep the operators so busy, they may not be able to handle all of the incoming signals. Similarly, if a burglar were to break into a building fifteen minutes before it was scheduled to open, the operator would probably dismiss any alarm as an employee having trouble disarming the system.

Finally, one should be aware of the peculiarities of some local annunciators. It would seem that if a burglar cut off the power to a bell or horn, and caused it to sound, the batteries would eventually wear down. If this were to happen, the whole home could, of course, be ransacked without sounding an alarm. That is why most sirens, bells and horns of a local system, run for about ten minutes before shutting themselves off, so that they may preserve battery power. Obviously, one could keep causing the alarm to go off, and the batteries would indeed run down eventually, but the chance of being caught increases with every alarm.

24

The Future Of Security Systems

As we've seen, most of the components of a modern burglar alarm system have several flaws that professional burglars can exploit to render the entire system useless. But homeowners want to know that they are safe from the professional burglar as well as the amateur, therefore cost is no longer the sole determining factor when they buy an alarm system.

Burglar alarm manufacturers are aware that some of their products are extremely easy to bypass, and some are going back to the drawing boards to try and devise new and more secure methods of burglary detection. Some of the newest methods are bio-mechanical, meaning that they are based on the characteristic idiosyncrasies of an individual's body. Still others use an ever-changing coding pattern, so that no repetitive motion can be copied by someone not authorized to enter. For example, there are key-pads on the market today that cannot be seen from any angle except straight-on, and the numbers are also scrambled into a different pattern every time. Thus, the same numeric code would use different buttons each time, so this would certainly nullify the Ultra-Violet ink method described in Chapter 13. Furthermore, magnetic cards are sometimes used instead of numeric

codes, to arm and disarm burglar alarms, but rarely in high-security situations, since they may simply be stolen from their owner.

Will the security industry ever stumble upon a technique that cannot be compromised? I don't know, but I'm afraid I have my doubts. If the alarm is bio-mechanical, an authorized person could be drugged and brought to the alarm panel, and the alarm could be allowed to check fingerprints, eye patterns, or whatever else the alarm needed for positive identification. A voice could also be recorded digitally, and played back, if the alarm checks for voice prints. For an alarm system that requires the input of a code, a person could be threatened with violence, beaten, drugged with sodium pentothal, or more humanely, hypnotized, so that he will reveal the code.

One possibility for increasing criminal detection would be to develop an entirely passive system, so that it could not be detected by burglars. Or, one could rig a system that did not arm until someone opened a door or window. That way, a burglar could not detect the presence of any alarm from the outside, and would probably deem it safe to enter. Also, the annunciator could be made to notify the neighbors silently, rather than blare throughout the neighborhood (on an easily defeated outdoor bell).

Some companies are now manufacturing stress sensors. These ultrasensitive units can measure any slight movement down to a few millionths of an inch. They sound an alarm when anyone walks on the stairs, the roof, or any other area. They are generally placed on structural beams, although they will also work if mounted to the wall. Of course, a stress sensor or any other component is useless if it is attached to a central processor that may be easily overcome.

There may come a day when security systems become so advanced that no one but authorized personnel can disarm them. There may come a time when we can arm our burglar alarms, and feel certain that we are safe from all types of criminals. But that time is not now, for the vast majority of alarms installed in this country are mere delays for the determined and experienced burglar. Alarm salesmen usually emphasize how secure you'll be and feel with a properly installed burglar alarm system. You may feel secure, but you will certainly be far from it. I sincerely hope that someday we'll all be safe in our homes, but I know, as you do now, that we have a long way to go.

"An excellent overview of all the current alarm systems."

— **Hustler**

"...the information is up-to-date, carefully presented... and has a broader appeal than the non-governmental B & E crowd."

—**Surveillant**

Any alarm system can be beaten. Criminals have gotten past everything from junkyard dogs to heat-sensing museum alarms. That doesn't mean alarms are worthless. It means anyone concerned with security needs to know how vulnerable these systems are.

Techniques of Burglar Alarm Bypassing gives you that knowledge. This book contains detailed descriptions of dozens of alarm systems: how they work, and how they can be defeated. Alarms covered include:
● Magnetic Switches ● Window Foil ● Sound and Heat Detectors ● Photoelectric Devices ● Guard Dogs ● Central Station Systems ● Closed-Circuit Television ● And much, much more!

Residential, commercial and high-security systems are described in plain English, with plenty of helpful illustrations.

Find out what you're missing — before you're missing *everything*. Get ***Techniques of Burglar Alarm Bypassing*** today!

ISBN 1-55950-032-8

90000

9 781559 500326